

Release Notes

Published
2021-04-22

Junos[®] OS 19.2R1 Release Notes

SUPPORTED ON

- ACX Series, EX Series, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, and SRX Series

HARDWARE HIGHLIGHTS

- SRX5K-SPC3 support Avira scan engine on antivirus module (SRX5400, SRX5600, and SRX5800)

SOFTWARE HIGHLIGHTS

- Support for BFD, BGP, IS-IS, and OSPF on IRB interfaces in EVPN-MPLS networks (EX Series)
- Support for control word in EVPN-VPWS (EX9200 Series and MX Series)
- Support for QSFP-100GE-DWDM2 transceiver (MX Series)
- MX2008 routers support in-chassis Junos node slicing (MX Series)
- Support for Synchronous Ethernet with ESMC on JNP10K-LC2101 (MX10008 and MX10016)
- PCE-initiated bypass LSPs (MX Series, PTX Series)
- Support for unified ISSU on abstracted fabric interfaces (MX Series)
- Support for fixed wireless access subscribers on BNGs (MX Series)
- Support for transferring accounting statistics files and router configuration archives using HTTP URL (MX Series)

- Packet Forwarding Engine statistics export using gNMI and JTI (MX Series, PTX1000 and PTX10000 routers, and QFX5100 and QFX5200 switches)
- Dynamic creation of segment routing LSPs using BGP protocol next hops (MX Series, PTX Series)
- gNMI support for Routing Engine statistics for JTI (QFX Series switches)
- Loopback firewall filter scale optimization (QFX5120)
- EVPN-VXLAN support (QFX10002-60C switches)
- Support for 512 ECMP next hops for BGP (QFX10000 switches)
- Support to configure micro-applications in a unified policy (SRX Series and vSRX)
- Application-level logging for AppQoE (SRX Series)
- Anti-Replay Window (SRX Series)

Release Notes: Junos[®] OS Release 19.2R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion

22 April 2021

Contents	Introduction 11
	Junos OS Release Notes for ACX Series 11
	New and Changed Features 12
	New and Changed Features: 19.2R1-S1 12
	New and Changed Features: 19.2R1 12
	Changes in Behavior and Syntax 16
	Interfaces and Chassis 17
	Junos OS XML, API, and Scripting 17
	Network Management and Monitoring 17
	VLAN Infrastructure 18
	Known Behavior 18
	General Routing 19
	Known Issues 20
	General Routing 21
	Interfaces and Chassis 24
	Resolved Issues 24
	Resolved Issues: 19.2R1-S1 25
	Resolved Issues: 19.2R1 25

Documentation Updates | 26

Installation and Upgrade Guide | 27

Migration, Upgrade, and Downgrade Instructions | 27

Upgrade and Downgrade Support Policy for Junos OS Releases | 27

Product Compatibility | 28

Hardware Compatibility | 29

Junos OS Release Notes for EX Series Switches | 30

New and Changed Features | 30

New and Changed Features: 19.2R1-S1 | 31

New and Changed Features: 19.2R1 | 31

Changes in Behavior and Syntax | 36

Network Management and Monitoring | 36

VLAN Infrastructure | 37

Known Behavior | 37

EVPN | 38

General Routing | 38

Platform and Infrastructure | 38

Known Issues | 38

General Routing | 39

Infrastructure | 40

Junos Fusion Enterprise | 41

Layer 3 Features | 41

Platform and Infrastructure | 41

Spanning Tree Protocols | 41

Resolved Issues | 42

Authentication and Access Control | 43

EVPN | 43

General Routing | 43

Infrastructure | 44

Interfaces and Chassis | 44

Layer 2 Ethernet Services | 45

Junos Fusion Enterprise | 45

Network Management and Monitoring | 45

Platform and Infrastructure | 45

Routing Protocols	46
Software Installation and Upgrade	46
Subscriber Access Management	46
Documentation Updates	47
Installation and Upgrade	47
Migration, Upgrade, and Downgrade Instructions	48
Upgrade and Downgrade Support Policy for Junos OS Releases	48
Product Compatibility	49
Hardware Compatibility	49
Junos OS Release Notes for Junos Fusion Enterprise	50
New and Changed Features	50
Changes in Behavior and Syntax	51
Known Behavior	52
Known Issues	52
Junos Fusion Enterprise	52
Resolved Issues	53
Resolved Issues: 19.2R1	53
Documentation Updates	54
Migration, Upgrade, and Downgrade Instructions	55
Basic Procedure for Upgrading Junos OS on an Aggregation Device	55
Upgrading an Aggregation Device with Redundant Routing Engines	57
Preparing the Switch for Satellite Device Conversion	57
Converting a Satellite Device to a Standalone Switch	59
Upgrade and Downgrade Support Policy for Junos OS Releases	59
Downgrading from Junos OS	59
Product Compatibility	60
Hardware and Software Compatibility	60
Hardware Compatibility Tool	60
Junos OS Release Notes for Junos Fusion Provider Edge	61
New and Changed Features	62
Spanning-Tree Protocols	62
Changes in Behavior and Syntax	62
Known Behavior	63

Known Issues | 63

Junos Fusion Provider Edge | 64

Resolved Issues | 64

Junos Fusion Provider Edge | 65

Junos Fusion Satellite Software | 65

Documentation Updates | 65

Migration, Upgrade, and Downgrade Instructions | 66

Basic Procedure for Upgrading an Aggregation Device | 66

Upgrading an Aggregation Device with Redundant Routing Engines | 69

Preparing the Switch for Satellite Device Conversion | 69

Converting a Satellite Device to a Standalone Device | 71

Upgrading an Aggregation Device | 73

Upgrade and Downgrade Support Policy for Junos OS Releases | 73

Downgrading from Junos OS Release 19.2 | 74

Product Compatibility | 74

Hardware Compatibility | 74

Junos OS Release Notes for MX Series 5G Universal Routing Platform | 75

New and Changed Features | 76

New and Changed Features: 19.2R1-S4 | 77

New and Changed Features: 19.2R1-S1 | 77

New and Changed Features: 19.2R1 | 78

Changes in Behavior and Syntax | 96

Interfaces and Chassis | 96

MPLS | 97

Network Management and Monitoring | 97

Routing Policy and Firewall Filters | 98

Services Applications | 98

Software Defined Networking | 98

Subscriber Management and Services | 98

VLAN Infrastructure | 99

Known Behavior | 100

General Routing | 100

Interfaces and Chassis | 101

Routing Protocols | 102

Known Issues | 102**EVPN | 103****Forwarding and Sampling | 103****General Routing | 104****Interfaces and Chassis | 108****Layer 2 Ethernet Services | 109****MPLS | 109****Platform and Infrastructure | 109****Routing Protocols | 110****Resolved Issues | 111****Application Layer Gateways (ALGs) | 112****Authentication and Access Control | 112****Class of Service (CoS) | 113****EVPN | 113****Flow-based and Packet-based Processing | 114****Forwarding and Sampling | 114****General Routing | 114****Infrastructure | 121****Interfaces and Chassis | 121****Layer 2 Features | 123****Layer 2 Ethernet Services | 123****MPLS | 123****Network Management and Monitoring | 124****Platform and Infrastructure | 125****Routing Policy and Firewall Filters | 125****Routing Protocols | 126****Services Applications | 127****Software Installation and Upgrade | 128****Subscriber Access Management | 128****User Interface and Configuration | 128****VPNs | 128****Documentation Updates | 129**

Migration, Upgrade, and Downgrade Instructions | 130**Basic Procedure for Upgrading to Release 19.2 | 131****Procedure to Upgrade to FreeBSD 11.x based Junos OS | 131****Procedure to Upgrade to FreeBSD 6.x based Junos OS | 133****Upgrade and Downgrade Support Policy for Junos OS Releases | 135****Upgrading a Router with Redundant Routing Engines | 136****Downgrading from Release 19.2 | 136****Product Compatibility | 137****Hardware Compatibility | 137****Junos OS Release Notes for NFX Series | 138****New and Changed Features | 138****Architecture | 139****Application Security | 139****Virtual Network Functions | 139****Changes in Behavior and Syntax | 140****Factory-default Configuration | 141****Known Behavior | 141****Interfaces | 141****Platform and Infrastructure | 142****Known Issues | 143****High Availability | 143****Interfaces | 143****Platform and Infrastructure | 144****Routing Protocols | 145****Virtual Network Functions (VNFs) | 145****Resolved Issues | 146****Interfaces | 146****Platform and Infrastructure | 146****Documentation Updates | 147****Migration, Upgrade, and Downgrade Instructions | 147****Upgrade and Downgrade Support Policy for Junos OS Releases | 148****Basic Procedure for Upgrading to Release 19.2 | 148****Product Compatibility | 150****Hardware Compatibility | 150**

Junos OS Release Notes for PTX Series Packet Transport Routers | 152

New and Changed Features | 153

New and Changed Features: 19.2R1-S4 | 154

New and Changed Features: 19.2R1-S1 | 154

New and Changed Features: 19.2R1 | 154

Changes in Behavior and Syntax | 160

What's Changed in Release 19.2R1-S5 | 161

What's Changed in Release 19.2R1 | 161

Known Behavior | 163

General Routing | 163

Interfaces and Chassis | 164

Known Issues | 164

General Routing | 165

Infrastructure | 166

Interfaces and Chassis | 166

Layer 2 Ethernet Services | 166

MPLS | 166

Routing Protocols | 166

Resolved Issues | 167

General Routing | 167

Infrastructure | 169

Interfaces and Chassis | 169

MPLS | 169

Platform and Infrastructure | 169

Routing Protocols | 169

Documentation Updates | 170

Installation and Upgrade Guide | 170

Migration, Upgrade, and Downgrade Instructions | 171

Basic Procedure for Upgrading to Release 19.2 | 171

Upgrade and Downgrade Support Policy for Junos OS Releases | 174

Upgrading a Router with Redundant Routing Engines | 174

Product Compatibility | 175

Hardware Compatibility | 175

Junos OS Release Notes for the QFX Series | 176

New and Changed Features | 177

New and Changed Features: 19.2R1-S1 | 177

New and Changed Features: 19.2R1 | 178

Changes in Behavior and Syntax | 186

Interfaces and Chassis | 186

Network Management and Monitoring | 187

Security | 187

Known Behavior | 188

EVPN | 188

General Routing | 188

Layer 2 Features | 189

Routing Protocols | 189

Known Issues | 190

EVPN | 190

General Routing | 191

Layer 2 Ethernet Services | 194

Layer 2 Features | 194

MPLS | 196

Platform and Infrastructure | 196

Routing Protocols | 196

Resolved Issues | 197

Resolved Issues: 19.2R1 | 197

Documentation Updates | 204

Installation and Upgrade guide | 204

Migration, Upgrade, and Downgrade Instructions | 205

Upgrading Software on QFX Series Switches | 205

Installing the Software on QFX10002-60C Switches | 208

Installing the Software on QFX10002 Switches | 208

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches | 209

Installing the Software on QFX10008 and QFX10016 Switches | 211

Performing a Unified ISSU | 215

Preparing the Switch for Software Installation | 216

Upgrading the Software Using Unified ISSU	216
Upgrade and Downgrade Support Policy for Junos OS Releases	218
Product Compatibility	219
Hardware Compatibility	219
Junos OS Release Notes for SRX Series	220
New and Changed Features	221
New and Changed Features: 19.2R1-S1	222
New and Changed Features: 19.2R1	222
Changes in Behavior and Syntax	231
Application Security	232
Ethernet Switching and Bridging	232
Flow-Based and Packet-Based Processing	232
Network Management and Monitoring	232
VPNs	233
Known Behavior	233
Flow-Based and Packet-Based Processing	234
J-Web	234
VPNs	234
Known Issues	235
Chassis Clustering	235
Flow-Based and Packet-Based Processing	235
J-Web	236
Platform and Infrastructure	236
User Firewall	236
VPNs	236
Resolved Issues	237
Application Firewall	237
Application Identification	237
Application Layer Gateways (ALGs)	237
Chassis Clustering	238
Flow-Based and Packet-Based Processing	238
Infrastructure	240
Interfaces and Routing	240
Intrusion Detection and Prevention (IDP)	241

Installation and Upgrade	241
J-Web	241
Logical Systems and Tenant Systems	242
Multiprotocol Label Switching (MPLS)	242
Network Address Translation (NAT)	242
Network Management and Monitoring	242
Platform and Infrastructure	242
Routing Policy and Firewall Filters	243
Unified Threat Management (UTM)	243
User Interface and Configuration	244
VPNs	244
Documentation Updates	245
Migration, Upgrade, and Downgrade Instructions	246
Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases	246
Product Compatibility	247
Hardware Compatibility	247
Upgrading Using ISSU	248
Licensing	248
Compliance Advisor	248
Finding More Information	249
Documentation Feedback	249
Requesting Technical Support	250
Self-Help Online Tools and Resources	250
Opening a Case with JTAC	251
Revision History	251

Introduction

Junos OS runs on the following Juniper Networks[®] hardware: ACX Series, EX Series, M Series, MX Series, NFX Series, PTX Series, QFabric systems, QFX Series, SRX Series, T Series, and Junos Fusion.

These release notes accompany Junos OS Release 19.2R1 for the ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- New and Changed Features | 12
- Changes in Behavior and Syntax | 16
- Known Behavior | 18
- Known Issues | 20
- Resolved Issues | 24
- Documentation Updates | 26
- Migration, Upgrade, and Downgrade Instructions | 27
- Product Compatibility | 28

These release notes accompany Junos OS Release 19.2R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [New and Changed Features: 19.2R1-S1 | 12](#)
- [New and Changed Features: 19.2R1 | 12](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for ACX Series Universal Metro Routers.

New and Changed Features: 19.2R1-S1

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Class of Service (CoS)

- **Support for class of service (CoS)(ACX6360 routers)**—Starting in Junos OS Release 19.2R1, ACX6360 routers support class of service (CoS) functionality.

CoS is the assignment of traffic flows to different service levels. Service providers can use router-based CoS features to define service levels that provide different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows.

[See [CoS on ACX Series Universal Metro Routers Features Overview](#).]

EVPN

- **EVPN support of VLAN ID ranges and lists in service provider style interface configurations (EX9200 switches, ACX5448 and MX Series routers, and vMX virtual routers)**—Starting in Junos OS Release 19.2R1, EX9200 switches, ACX5448 and MX Series routers, and vMX virtual routers support the use of VLAN ID ranges and lists in a service provider style interface configuration, which must be referenced in an EVPN routing instance. This configuration is supported with the following EVPN environments, services, and features:
 - Environments:

- EVPN with VXLAN encapsulation
- EVPN with MPLS encapsulation
- VLAN bundle service:
 - E-LAN
 - E-Tree
 - E-Line
- Feature:
 - EVPN multihoming:
 - All-active
 - Single-active
 - Singlehoming

[See [VLAN ID Ranges and Lists in an EVPN Environment](#).]

Interfaces and Chassis

- **Support for 100-Mbps and 1-Gbps speeds on Tri-Rate Copper SFP (ACX5448 routers)**—Starting in Junos OS Release 19.2R1, ACX5448 routers support 100-Mbps and 1-Gbps speeds on Tri-Rate Copper SFP optics (part number 740-013111).

NOTE: 100-Mbps speed is supported only on ports xe-0/0/24 through xe-0/0/47.

10-Mbps speed is not supported on Tri-Rate Copper SFP due to hardware limitations.

- To set the speed for the optics, issue the **set interfaces *interface-name* speed auto** command. [See [Speed](#) for more details.]
- To enable autonegotiation, issue the **set interfaces *interface-name* gigether-options auto-negotiation** command. [See [auto-negotiation](#).]

Junos Telemetry Interface

- **Support for LSP statistics on JTI (ACX6360)**—Starting with Junos OS Release 19.2R1, you can provision the LSP statistics sensor using the resource path **/junos/services/label-switched-path/usage/** to monitor per-MPLS LSP statistics on the ACX6360 router and export telemetry data through Junos telemetry interface (JTI) to external collectors. You can stream data at configurable intervals through gRPC without involving polling.

JTI support is only for RSVP LSPs.

Statistics that are streamed are similar to the output displayed by the operational mode command **show mpls lsp bypass statistics**.

To provision a sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

To enable statistics for export from the Junos OS, include the **sensor-based-stats** statement at the **[edit protocols mpls]** hierarchy level.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Specify Routing Instance for JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 19.2R1, you can specify the routing instance to use for remote procedure call (gRPC) services. Include the **routing-instance instance-name** at the **[edit system services extension-service request-response grpc]** hierarchy level. The routing instance name specified should match the name of the existing routing instance, such as a name configured under the **[routing-instances]** hierarchy level or **mgmt_junos** if **system management-instance** is configured (the dedicated management routing instance).

Configuring the routing instance lets you choose the VRF for gRPC services. When the routing instance is not configured, the default behavior is that all gRPC-related services are available through the management **fxp0/em0** interface.

Layer 3 Features

- **Support for Layer 3 unicast features (ACX 6360)**—Starting in Junos OS Release 19.2R1, ACX routers support the following Layer 3 forwarding features for unicast IPv4 and IPv6 traffic:
 - Basic IPv6 forwarding
 - Virtual router (VRF-lite) for both IPv4 and IPv6
 - Layer 3 subinterfaces support for both IPv4 and IPv6
 - VRF-lite, subinterfaces, and IPv6 forwarding support on link aggregation groups (LAGs)
 - Statistics support for Layer 3 subinterfaces
 - 32-way equal-cost multipath (ECMP)
 - Centralized Bidirectional Forwarding Detection (BFD)
 - IPv4 Layer 3 protocols:
 - OSPF
 - IS-IS
 - BGP
 - IPv6 Layer 3 protocols:

- OSPFv3
- RIPng

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (ACX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data model when you include the **action-expand** extension statement in the option or statement definition and reference a script that handles the logic. The **action-expand** statement must include the **script** child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

Software Installation and Upgrade

- **Zero Touch Provisioning (ACX5448)**—Starting in Junos OS Release 19.2R1, Zero Touch Provisioning (ZTP) automates the provisioning of the device configuration and software image with minimal manual intervention on management interface **em0**.

When you physically connect a router to the network and boot it with a factory configuration, the router upgrades the Junos OS software image automatically and automatically installs a configuration file from the network through the management interface.

[See [Zero Touch Provisioning](#).]

System Management

- **Support for transferring accounting statistics files and router configuration archives using HTTP URL (ACX Series)**—Starting in Junos OS Release 19.2R1, you can transfer accounting statistics files and router configuration archives to remote servers by using an HTTP URL. In addition to SCP and FTP, the following HTTP URL will be supported under the **archive-sites** statement:

http://username@host:url-path password password

- To transfer accounting statistics files, configure **archive-sites** under **[edit accounting-options file <filename>]** hierarchy.
- To transfer router configuration archival, configure **archive-sites** under **edit system archival configuration** hierarchy.
- To view the statistics of transfer attempted, succeeded, and failed, use the **show accounting server statistics archival-transfer** command.
- To clear the statistics of transfer attempted, succeeded, and failed, use the **clear accounting server statistics archival-transfer** command.

[See [archive-sites](#), [Backing Up Configurations to an Archive Site](#), [show accounting server statistics archival-transfer](#), and [clear accounting server statistics archival-transfer](#)].

- **Precision Time Protocol (PTP) Transparent Clock with IPv6 Transport (PTX10001-20C and ACX6360-OR devices)**—Starting with Junos OS Release 19.2R1, PTP uses IPv6 transport to synchronize clocks throughout a packet-switched network. With a transparent clock, the PTP packets are updated with the residence time as the packets pass through the switch. There is no master/slaved designation. End-to-end transparent clocks are supported. With an end-to-end transparent clock, only the residence time is included. The residence time can be sent in a one-step process, which means that the timestamps are sent in one packet.

You can configure the transparent clock at the **[edit protocols ptp]** Junos OS CLI hierarchy.

[See [Understanding Transparent Clocks in Precision Time Protocol](#).]

SEE ALSO

[What's Changed | 16](#)

[Known Limitations | 18](#)

[Open Issues | 20](#)

[Resolved Issues | 24](#)

[Documentation Updates | 26](#)

[Migration, Upgrade, and Downgrade Instructions | 27](#)

[Product Compatibility | 28](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 17](#)
- [Junos OS XML, API, and Scripting | 17](#)
- [Network Management and Monitoring | 17](#)
- [VLAN Infrastructure | 18](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the ACX Series routers.

Interfaces and Chassis

- **Monitoring information available only in trace log (ACX Series)**—In Junos OS Release 19.2R1 and later, the Ethernet link fault management daemon (lfmd) in the peer router stops monitoring the locally occurred errors until ISSU completes. You can view the monitoring-related details only through the trace log file.

Junos OS XML, API, and Scripting

- **Mandatory configurations and omission of <database-status-information> tag in platforms supporting Open ROADM standard (ACX6160-T)**—Starting in Junos OS Release 19.2R1, it is mandatory to apply **rfc-compliant** option at the [edit system services netconf] hierarchy level and **unhide** option at the [edit system services netconf unified] hierarchy level. Also, <database-status-information> tag is omitted for <get> RPC query.

[See [<get>](#) and [netconf](#).]

Network Management and Monitoring

- **The show system schema command and <get-yang-schema> RPC require specifying an output directory (ACX Series)**—Starting in Junos OS Release 19.2R1, when you issue the **show system schema** operational mode command in the CLI or execute the <get-yang-schema> RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the <output-directory> element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type empty (ACX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are only supported when executing the RPC in a NETCONF or Junos XML protocol session, and the value passed to the action script is the string '**none**'.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

VLAN Infrastructure

- **Specifying a descending VLAN ID range (ACX5448 routers)**—In Junos OS releases prior to Junos OS Release 19.2R1, the system accepts a descending range—for example, 102-100, with the **vlan-id-range** configuration statement in the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy.

Starting with Junos OS Release 19.2R1, the system considers a descending range specified with **vlan-id-range** to be invalid and raises an error if you try to commit this configuration.

SEE ALSO

What's New 12
Known Limitations 18
Open Issues 20
Resolved Issues 24
Documentation Updates 26
Migration, Upgrade, and Downgrade Instructions 27
Product Compatibility 28

Known Behavior

IN THIS SECTION

- [General Routing | 19](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the ACX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- ACX6360-OR Telemetry infrastructure does not support the interface-filtering capability. Therefore, after you enable a particular sensor for telemetry, it is turned on for all the interfaces. [PR1371996](#)
- For the et interface, only PRE_FEC_SD defect is raised no OTN alarm is raised. [PR1371997](#)
- **static-cak** encryption does not work between two ACX-OX transponder nodes. [PR1389802](#)
- For ACX6360 TIC, the beacon port-range needs to be updated to 0-7 instead of 0-15. [PR1399335](#)
- When timing configuration and corresponding interface configuration is flapped for multiple times in iteration, PTP is stuck in "INITIALIZE" state where the ARP for the neighbor is not resolved. In issue state, BCM hardware block get into inconsistency state, where the lookup is failing. [PR1410746](#)
- Snake traffic fails because of the static MAC address assigned for interface. Static MAC address on interface is not supported in ACX Series routers. [PR1427132](#)
- When an end device (fan tray CPLD) i2c line is grounded or pulled low, the other device fails to write or read. As a workaround, verify the isolation functionality through software simulation when the device is in the problem state. But in this case where we grounded one of the fan tray CPLD i2c line to verify the failed test case, then entire circuit will get stalled and it leads to write fail for other devices also such as the PEM, temp sensors. [PR1427222](#)
- Multicast packets are flooded in a BD if snooping is not enabled. If interfaces x and y belong to a BD, then all multicast packets will be flooded to both x and y interface. If packets are received from interface x, packets will be flooded to x & y in ingress but discarded in the egress path for interface x because the packet is received from the same interface. But these packets are also counted in the VOQ and hence more queue statistics are seen. This is a known hardware limitation. **monitor interface xe-0/0/30**Input packets: 177958 (64 pps) [0]Output packets: 357306 (128 pps) [0] **monitor interface xe-0/0/12**Input packets: 361161 (128 pps) [642]Output packets: 179878 (63 pps) [320] root@rioxd-p2a-a> show interfaces queue xe-0/0/30 Queue: 0, Forwarding classes: best-effortQueued:Packets : 544032 192 pps. => Sum of 64 + 128pps root@rioxd-p2a-a> show interfaces queue xe-0/0/12 Queue: 0, Forwarding classes: best-effortQueued:Packets : 550929 192 pps. => Sum of 64 + 128pps [PR1429628](#)
- Any packet greater than MTU size will be accounted as oversized packets. Packets exceeding MTU sizes are not considered for Jabber check. [PR1429923](#)
- Even the system LED glows during halt state. [PR1430129](#)
- Packets dropped because MTU checks in the output interface are not accounted for MTU errors. All packets above MTU size are accounted for oversized packets in the input interface. [PR1430446](#)
- 1G interfaces are shown as 'xe'. Therefore, the cosmetic issue is observed with respect to auto-negotiation parameters though there is no impact on functionality. [PR1430835](#)
- BCM SDK do not support statistics. The routes get re-installed on a periodic basis and SDK does not support statistics unless Flex mode is moved in KBP. [PR1435579](#)
- The logical interface statistics in ACX5448 displays the full packet size similar to the behaviour in ACX5000 Series. [PR1439124](#)

- The time taken to copy DNX file through a WAN interface is more compared to ACX5000. [PR1439960](#)
- The hold timer expiry is common across all platforms. It is not specific to RIO platforms. [PR1439980](#)
- Remote loopback is not supported on RIO-X. [PR1443517](#)

SEE ALSO

What's New	 12
What's Changed	 16
Open Issues	 20
Resolved Issues	 24
Documentation Updates	 26
Migration, Upgrade, and Downgrade Instructions	 27
Product Compatibility	 28

Known Issues

IN THIS SECTION

- [General Routing](#) | [21](#)
- [Interfaces and Chassis](#) | [24](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for the ACX Series Universal Metro Routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- Forwarding when using non-existing SSM map source address in IGMPv3 instead of pruning. This is a day 1 design issue which needs to be redesigned. The impact is more, But definitely this needs some soaking time in DCB before it gets ported in previous versions. [PR1126699](#)
- When ACX 2100 and 2200 routers are used as ingress PE routers for L2circuit connections, and the PE-CE interface (UNI) is an aggregated Ethernet interface, then upon MPLS path switchover, the traffic might be silently dropped or discarded. [PR1194551](#)
- The maximum number of logical interfaces (IFLs) on the ACX5000 line of routers has been increased from 1000 to 4000. [PR1229492](#)
- When Layer 3 packets are classified, DiffServ code points are not preserved but are getting lost at the egress interface because of a chipset limitation. [PR1322142](#)
- On ACX5000 platforms with Junos OS 16.2 onwards, the fxpc process might use high CPU. This issue can occur after an upgrade in some cases. [PR1360452](#)
- On ACX1x00/ACX2x00/ACX4x00 running in 15-releases previous to Junos OS Release 15.1R8, when configuring **mac-table-size** under **bridge-domain**, an incorrect commit error appears, not allowing the commit to succeed. [PR1364811](#)
- The switchover time observed is more than 50ms under certain soak test conditions with an increased scale with a multi-protocol multi-router topology. [PR1387858](#)
- On ACX5000 running Junos OS Release 17.3 and later releases, the Packet Forwarding Engine syslog frequently shows the following error messages: **acx_cos_tcp_bind_queues:736 parent acx_cos_tcp_ifd for ifd:ae0 doesn't exist for ifl:549**. In Junos OS Release 17.3R3-S1, the error logs appear only from time to time, and this can be related with an interface flap. In Junos OS Release 18.1R3, the logs appear constantly, without any interface flap. This message is related to HCOS checking (even without HCOS configured). In the software fix, check if the aggregate interface has HCOS configured or not. If not, return gracefully from this function without throwing this error. This is a harmless message. [PR1392088](#)
- IGMP packets over Layer 2 Circuit with control word are dropped in ACX5048. [PR1394301](#)
- On ACX1000, ACX2000, ACX4000, ACX5048, and ACX5096 platforms, after a new child logical interface with VLAN and filter is added on an aggregated Ethernet IFD or changing the VLAN ID of a child IFL with filter, traffic over the aggregated Ethernet physical interface might get filtered with that filter on the child IFL. For example: ae-0/0/0 is an physical interface and ae-0/0/0.100 is an llogical interface. [PR1407855](#)
- Clock Class value is wrong in Default Data (show ptp clock) when the slave interface is down in PTP-OC device. [PR1416421](#)
- On ACX5448 devices, the ZTP process will proceed with the image upgrade even in situations when there is a mismatch in the platform name of the software image stored on FTP/ZTP servers and the actual platform on which the ZTP process is being run. [PR1418313](#)

- Hardware-based fragmentation or reassembly is not supported. Software-based fragmentation rates are going to be extremely slow depending CPU load. [PR1419371](#)
- On ACX5000 platforms, thigh CPU usage on the fxpc process might be seen under rare condition if parity errors are detected in devices. It has no direct service or traffic impact. However, since CPU utilization is high during this issue, there are some side effects. For example, it could impact time-sensitive features such as BFD. [PR1419761](#)
- Packets transmitted in a queue are not as expected when testing IEEE-802.1ad inner classifier at the ingress and IEEE-802.1ad rewrite at the egress with various events. [PR1422515](#)
- The input packets account for all the frames that are coming in, including the oversized frames. Whereas oversized frame counter only accounts for oversized frames. [PR1425748](#)
- Because of the BCM sdk design, EEDB hardware entry is not freed for unicast next-hop creation. This leads to resource leakage and is not allowing to higher scale. [PR1426734](#)
- Error messages can be seen sometimes if the optics is being unplugged in between the eeprom read. This is expected and will not impact any functionality. [PR1429016](#)
- Multiple hardware i2c failure observed because of intermittent layer 2 circuit access failure on main board switches. [PR1429047](#)
- Packet rates are not seen for aggregated Ethernet logical interface. [PR1429590](#)
- Traffic loss is seen if the configuration has /128 prefix routes and it is limited to /128 only. Its due to the known issue tracked in PR 1445231. [PR1429833](#)
- Any packet greater than the MTU size will be accounted as oversized packets. Packets exceeding the MTU sizes are not considered for jabber check. [PR1429923](#)
- This is the expected behavior across all ACX platforms. Even the system LED glows during halt state. [PR1430129](#)
- These are initial transient messages seen and does not have any functional impact. [PR1430355](#)
- Packets dropped due to MTU checks in the output interface are not accounted for MTU errors. All packets above MTU size are accounted for Oversized-packets in the input interface. [PR1430446](#)
- If L2VPN sessions have OAM control-channel option set to router-alert-label, the no-control-word option in L2VPN should not be used for BFD sessions to come up. [PR1432854](#)
- Timing on 1G, performance is not in par compared with 10G, compensation is done to bring the mean value under class-A but the peak to peak variations are high and can go beyond 100ns. It has a latency variation with peak to peak variations of around 125ns-250ns (that is, 5-10 percent of the mean latency introduced by the each phy which is of around 2.5us) without any traffic. [PR1437175](#)
- These errors can be seen if CFP2 optics are not plugged in. [PR1438039](#)
- 1PPS performance metrics (class A) of G.8273.2 are not met for 1G interfaces because of the variable latency added by the Vitesse PHY. [PR1439231](#)

- In a certain test condition, it is observed that L2VPN at a scale of 16000 had issues when all were brought down and up. [PR1439471](#)
- With an asymmetric network connection (for example, 10G MACsec port connected to 10G channelized port), high and asymmetric T1 and T4 time errors are seen which introduces a high 2 way time error. This introduces different CF updates in forward and reverse paths. [PR1440140](#)
- By default mgmt interface speed always shows as 1000Mbps in Junos OS. [PR1440675](#)
- With MACsec feature enabled and introduction of traffic, the peak to peak value varies with the percentage of traffic introduced. [PR1441388](#)
- Recovery of Junos OS volume is not possible from OAM menu. [PR1446512](#)
- SyncE Jitter tolerance test fails for MACsec ports. For SyncE with MACsec there seems to be additional framing header and footer that would get added by the MACsec protocol. The impact of this on the jitter test is not obvious and look undefined in the standards and not qualifiable with a single DUT and Calnex. [PR1447296](#)
- Drop profile maximum threshold might not be reached to its limit when the packet size is other than 1000 bytes. This is due to current design limitation. Making design changes are high risk at this point of time, Hence, The Junos OS Releases 19.2R1-S1, 19.2R(x), and 19.3(x) will not have fix for this issue. [PR1448418](#)
- If the client et- interface is up and transportd state is in init state, restart transportd process to get the state updated to normal. This scenario is not seen in normal operation but seen when interfaces are deleted and re-created and configurations are applied. [PR1449937](#)
- Red drops seen on the 25G channelized aggregated Ethernet interfaces after some events (deactivate, activate etc) on the PEER box. [PR1450674](#)
- For the et ports, some output power might be seen even after disabling the interface. This will not have any functional impact as the bcmport is getting disabled on the interface and the link goes down fine. [PR1452323](#)
- Incorrect operating state is displayed in SNMP trap message when a FAN tray is removed. [PR1455577](#)
- FAN numbering is not the same in the outputs of the following configuration statements **show chassis fan** and **show snmp mib walk jnxContentsDescr**. [PR1456589](#)

Interfaces and Chassis

- When an unnumbered interface is binding to an interface that has more than one IP address and one of the IP addresses is deleted, the family inet of the unnumbered interface might be deleted. The issue results in traffic loss for all the services that rely on the family inet of the unnumbered interface. Configure **preferred-source-address** on the unnumbered interface to prevent deletion of the IP address, thereby avoiding the deletion of the family inet of the unnumbered interface. [PR1412534](#)

SEE ALSO

[What's New | 12](#)

[What's Changed | 16](#)

[Known Limitations | 18](#)

[Resolved Issues | 24](#)

[Documentation Updates | 26](#)

[Migration, Upgrade, and Downgrade Instructions | 27](#)

[Product Compatibility | 28](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 19.2R1-S1 | 25](#)
- [Resolved Issues: 19.2R1 | 25](#)

This section lists the issues fixed in Junos OS Release 19.2R1 for the ACX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Resolved Issues: 19.2R1-S1

General Routing

- Link Fault Signaling (LFS) do not work on ACX5448, ACX5410, ACX5440, and 100-Gigabit Ethernet interfaces. [PR1401718](#)
- In an ACX5448 platforms, when the Packet Forwarding Engine failed to allocate packet buffer, portion of packet memories might not be free. [PR1442901](#)

Resolved Issues: 19.2R1

Class of Service (CoS)

- The error message **STUCK_BUFF : port_sp not empty for port 35 sp 1 pkts:1** is seen when a lag bundle is configured with 64 lag links.. [PR1346452](#)

General Routing

- The 1G copper module interface shows "Link-mode: Half-duplex". [PR1286709](#)
- On an ACX ring topology, after link between ACX and MX flaps, VPLS RI on PE (MX) has no MAC of CE over I2circuit. [PR1360967](#)
- ACX5000: **fpc0 (acx_rt_ip_uc_lpm_install:LPM route add failed** error) Reason : Invalid parameter after configuring lpm-profile. [PR1365034](#)
- ACX5448: **LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified** prints while committing on configuration prompt. [PR1376665](#)
- On ACX5448, channelized ET interface of 25-Gigabit interface will not come up after chassis-control restart. [PR1379288](#)
- ACX 5448:100 Gigabit link FEC enabled by default on 100G LR4. [PR1389518](#)
- On ACX Series platforms, the **forwarding-option dhcp-relay forward-only** command stops working and the DHCP packets are dropped. [PR1392261](#)
- On ACX5048, RPM RFC 2544 benchmarking test failed to start. [PR1395730](#)
- CFM adjacency is not going down with distinct intervals. [PR1397883](#)
- Dynamic tunnels are not supported on ACX Series routers. [PR1398729](#)
- VLAN tagged traffic arriving on VPLS interface might get dropped. [PR1402626](#)
- ot/et interface is not created when invalid speed is configured. [PR1403546](#)
- ACX 5448: TrTCM Policer configuration parameters are as per RFC4115. [PR1405798](#)
- The **show services inline stateful-firewall flow** or **show services inline stateful-firewall flow extensive** command might cause a memory leak. [PR1408982](#)
- ACX Series routers drop DNS responses that contain an underscore. [PR1410062](#)

- VPLS traffic might stop across ACX5000 with the aggregated Ethernet interface. [PR1412042](#)
- Junos PCC might reject PCUpdate/PCCreate message if there is metric type other than type 2. [PR1412659](#)
- Number of inet-arp policers implemented on ACX5000 has been increased from 16 to 64. [PR1413807](#)
- Swap memory is not initialized on boot on ACX5048. [PR1415898](#)
- Commit error while configuring firewall with term having log/syslog and accept actions. [PR1417377](#)
- CoS table error can sometimes cause traffic outages and SNMP timeouts if the optic is plugged out and inserted back. [PR1418696](#)
- Slow copy image speed to ACX5448. [PR1422544](#)

SEE ALSO

[What's New | 12](#)

[What's Changed | 16](#)

[Known Limitations | 18](#)

[Open Issues | 20](#)

[Documentation Updates | 26](#)

[Migration, Upgrade, and Downgrade Instructions | 27](#)

[Product Compatibility | 28](#)

Documentation Updates

IN THIS SECTION

- [Installation and Upgrade Guide | 27](#)

This section lists the errata and changes in Junos OS Release 19.2R1 for the ACX Series documentation.

Installation and Upgrade Guide

- **Veriexec explained (ACX Series)**—Verified Exec (also known as veriexec) is a file-signing and verification scheme that protects the Junos operating system (OS) against unauthorized software and activity that might compromise the integrity of your device. Originally developed for the NetBSD OS, veriexec was adapted for Junos OS and enabled by default from Junos OS Release 7.5 onwards.

[See [Veriexec Overview](#).]

SEE ALSO

What's New	 12
What's Changed	 16
Known Limitations	 18
Open Issues	 20
Resolved Issues	 24
Migration, Upgrade, and Downgrade Instructions	 27
Product Compatibility	 28

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases](#) | 27

This section contains the upgrade and downgrade support policy for Junos OS for the ACX Series Router. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases

provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

SEE ALSO

[What's New | 12](#)

[What's Changed | 16](#)

[Known Limitations | 18](#)

[Open Issues | 20](#)

[Resolved Issues | 24](#)

[Documentation Updates | 26](#)

[Product Compatibility | 28](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 29](#)

Hardware Compatibility

To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on ACX Series routers in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

What's New	 12
What's Changed	 16
Known Limitations	 18
Open Issues	 20
Resolved Issues	 24
Documentation Updates	 26
Migration, Upgrade, and Downgrade Instructions	 27

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- New and Changed Features | 30
- Changes in Behavior and Syntax | 36
- Known Behavior | 37
- Known Issues | 38
- Resolved Issues | 42
- Documentation Updates | 47
- Migration, Upgrade, and Downgrade Instructions | 48
- Product Compatibility | 49

These release notes accompany Junos OS Release 19.2R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- New and Changed Features: 19.2R1-S1 | 31
- New and Changed Features: 19.2R1 | 31

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for the EX Series.

NOTE: The following EX Series switches are supported in Release 19.2R1: EX2300, EX2300-C, EX3400, EX4300, EX4600-40F, EX4650, EX9200, EX9204, EX9208, EX9214, EX9251, and EX9253.

New and Changed Features: 19.2R1-S1

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Authentication, Authorization, and Accounting (AAA)

- **802.1X authentication (EX4650 switches)**—Starting with Junos OS Release 19.2R1, EX4650 switches support port-based network access control using 802.1X authentication as defined in the IEEE 802.1X standard.

[See [802.1X for Switches Overview](#).]

Dynamic Host Configuration Protocol

- **Support for DHCP snooping and other access port security features on private VLANs (EX4300-MP switches and Virtual Chassis)**—Starting in Junos OS Release 19.2R1, you can enable DHCP snooping for security purposes on access ports that are in a private VLAN (PVLAN). You can also protect those ports with DHCP options, dynamic ARP inspection (DAI), IP source guard, and neighbor discovery inspection.

[See [Putting Access Port Security on Private VLANs](#).]

EVPN

- **Support for BFD, BGP, IS-IS, and OSPF on IRB interfaces in EVPN-MPLS networks (EX series)**—Starting with Junos OS Release 19.2R1, you can configure Bidirectional Forwarding Detection (BFD), BGP, IS-IS, and OSPF routing protocols on the IRB interface in an EVPN-MPLS network to route and forward EVPN traffic. This feature supports single-homed, single-active, and all-active multihomed networks.

[See [EVPN with IRB Solution Overview](#).]

- **EVPN support of VLAN ID ranges and lists in service provider style interface configurations (EX9200 switches)**—Starting in Junos OS Release 19.2R1, EX9200 switches, ACX5448 and MX Series routers, and vMX virtual routers support the use of VLAN ID ranges and lists in a service provider style interface

configuration, which must be referenced in an EVPN routing instance. This configuration is supported with the following EVPN environments, services, and features:

- Environments:
 - EVPN with VXLAN encapsulation
 - EVPN with MPLS encapsulation
- VLAN bundle service:
 - E-LAN
 - E-Tree
 - E-Line
- Features:
 - EVPN multihoming:
 - All-active
 - Single-active
 - Singlehoming

[See [VLAN ID Ranges and Lists in an EVPN Environment](#).]

- **Support for control word in EVPN-VPWS (EX9200 switches)**—Starting with Junos OS Release 19.2R1, Junos OS supports the insertion of a control word between the label stack and the MPLS payload in a network with EVPN-VPWS service. This feature prevents a transit device from delivering out-of-order packets as a result of the device's load-balancing hashing algorithm. When you enable the control word feature on a PE device, the PE device advertises support for a control word. If all the PE devices in an EVI on the EVPN-VPWS serviced network support control word, then the PE device inserts a control word between the label stack and the L2 header in the packet thus preventing the packet from being misidentified by transit devices.

[See [Control Word for EVPN-VPWS](#).]

JWeb

- **Support for EX4650 switches**—Starting in Junos OS Release 19.2R1, you can use J-Web to configure, monitor, and manage EX4650 switches.

To configure the EX4650 switch using the J-Web interface, you must connect the cable to the port labeled **CON** on the rear panel of the switch.

NOTE: In J-Web, the chassis viewer displays only the standalone EX4650 switches view. It does not display the Virtual Chassis configuration because the EX4650 switch does not support the Virtual Chassis configuration.

[See [Dashboard for EX Series Switches](#) and [Connecting and Configuring an EX Series Switch \(J-Web Procedure\)](#).]

Layer 2 Features

- **L2PT support (EX4300 multigigabit switches)**—Starting with Junos OS Release 19.2R1, you can configure Layer 2 protocol tunneling (L2PT) for the following protocols on EX4300 multigigabit switches (EX4300-48MP models): CDP, E-LMI, GVRP, IEEE 802.1X, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, STP (including RSTP and MSTP), UDLD, VSTP, and VTP.

[See [Layer 2 Protocol Tunneling](#).]

Multicast

- **Support for multicast traffic counters (EX4300, EX4300-MP, EX4300 Virtual Chassis)**—Starting with Junos OS Release 19.2R1, you can use firewall filters to count packets and check the bandwidth of multicast traffic received by a host from a particular source and group in a routing instance. To enable this feature, include the **multicast-statistics** statement at the **[edit system packet-forwarding-options]** hierarchy level. To check the packet count and bandwidth for each multicast route, use the **show multicast route extensive** command.

[See [multicast-statistics \(system-packet forwarding\)](#).]

- **IGMP snooping with private VLANs (EX4300 multigigabit switches)**—Starting in Junos OS Release 19.2R1, EX4300 multigigabit switches (EX4300-48MP models) support IGMP snooping with private VLANs (PVLANS). A PVLAN consists of secondary isolated and community VLANs configured within a primary VLAN. Without IGMP snooping support on the secondary VLANs, switches receive multicast streams on a primary VLAN and flood them to the secondary VLANs. This feature extends IGMP snooping on a primary VLAN to its secondary VLANs to further constrain multicast streams only to interested receivers on PVLANS. When you enable IGMP snooping on a primary VLAN, you implicitly enable it on all secondary VLANs, and the secondary VLANs learn the multicast group information on the primary VLAN.

NOTE: Ports in a secondary VLAN cannot be used as IGMP multicast router interfaces. Secondary VLANs can receive multicast data streams ingressing on promiscuous trunk ports or inter-switch links acting as multicast router interfaces.

[See [IGMP Snooping Overview](#).]

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (EX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data model when you include the **action-expand** extension statement in the option or statement definition and reference a script that handles the logic. The **action-expand** statement must include the **script** child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

Port Security

- **Stateless address autoconfiguration (SLAAC) snooping (EX2300, EX3400, EX4300, and Virtual Chassis)**—Starting in Junos OS Release 19.2R1, Junos OS supports SLAAC snooping on EX2300, EX2300 VC, EX3400, EX3400 VC, EX4300, and EX4300 VC. IPv6 clients using SLAAC for dynamic address assignment are validated against the SLAAC snooping binding table before being allowed access to the network.

[See [IPv6 Stateless Address Autoconfiguration \(SLAAC\) Snooping](#).]

- **Fallback PSK for Media Access Control Security (MACsec) (EX Series)**—Starting in Junos OS Release 19.2R1, fallback PSK for MACsec is supported on EX Series routers that support MACsec. The fallback PSK provides functionality to establish a secure session in the event that the primary PSKs on each end of a MACsec-secured link do not match.

[See [Configuring MACsec on EX, SRX and Fusion Devices](#).]

- **Support for 802.1X authentication on private VLANs (PVLANS) (EX4300-48MP switches and Virtual Chassis)**—Starting in Junos OS Release 19.2R1, you can enable 802.1X (dot1x) authentication for security purposes on access ports that are in a PVLAN.

PVLANS provide Layer 2 isolation between ports within a VLAN, splitting a broadcast domain into multiple discrete broadcast subdomains by creating secondary VLANs. PVLANS are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts.

Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a DHCP server.

On a switch that is configured with both 802.1X authentication and PVLANS, when a new device is attached to the PVLAN network, the device is authenticated and then is assigned to a secondary VLAN based on the PVLAN configuration or RADIUS profile. The device then obtains an IP address and receives access to the PVLAN network.

[See [Using 802.1X Authentication and Private VLANs Together on the Same Interface.](#)]

- **Media Access Control security with 256-bit cipher suite (EX4300)**—Starting in Junos OS Release 19.2R1, the GCM-AES-256 cipher suite for MACsec in static CAK mode is supported on the 2-port QSFP+/1-port QSFP28 uplink module for EX4300-48MP switches. The GCM-AES-256 cipher suite has a maximum key length of 256 bits and is also available with extended packet numbering (GCM-AES-XPB-256).

[See [Understanding Media Access Control Security \(MACsec\).](#)]

- **Support for MACsec PSK keychain (EX9253)**—Starting in Junos OS Release 19.2R1, EX9253 switches support MACsec PSK chains hitless rollover and Key Agreement Protocol Fail Open mode.

[See [Configuring MACsec on EX, SRX and Fusion Devices.](#)]

System Management

- **Support for transferring accounting statistics files and router configuration archives using HTTP URL (EX Series)**—Starting in Junos OS Release 19.2R1, you can transfer accounting statistics files and router configuration archives to remote servers by using an HTTP URL. In addition to SCP and FTP, the following HTTP URL will be supported under the **archive-sites** statement:

`http://username@host:url-path password password`

- To transfer accounting statistics files, configure **archive-sites** under **[edit accounting-options file <filename>]** hierarchy.
- To transfer router configuration archival, configure **archive-sites** under **edit system archival configuration** hierarchy.
- To view the statistics of transfer attempted, succeeded, and failed, use the **show accounting server statistics archival-transfer** command.
- To clear the statistics of transfer attempted, succeeded, and failed, use the **clear accounting server statistics archival-transfer** command.

[See [archive-sites](#), [Backing Up Configurations to an Archive Site](#), [show accounting server statistics archival-transfer](#), and [clear accounting server statistics archival-transfer](#)].

SEE ALSO

[What's Chnaged](#) | 36

[Known Behavior](#) | 37

[Open Issues](#) | 38

[Resolved Issues | 42](#)

[Documentation Updates | 47](#)

[Migration, Upgrade, and Downgrade Instructions | 48](#)

[Product Compatibility | 49](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Network Management and Monitoring | 36](#)
- [VLAN Infrastructure | 37](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the EX Series.

Network Management and Monitoring

- **The `show system schema` command and `<get-yang-schema>` RPC require specifying an output directory (EX Series)**—Starting in Junos OS Release 19.2R1, when you issue the `show system schema` operational mode command in the CLI or execute the `<get-yang-schema>` RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the `<output-directory>` element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type `empty` (EX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are only supported when executing the RPC in a NETCONF or Junos XML protocol session, and the value passed to the action script is the string `'none'`.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

VLAN Infrastructure

- **Specifying a descending VLAN ID range (EX9200 switches)**—In Junos OS releases prior to Junos OS Release 19.2R1, the system accepts a descending range—for example, 102-100, with the **vlan-id-range** configuration statement in the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy.

Starting with Junos OS Release 19.2R1, the system considers a descending range specified with **vlan-id-range** to be invalid and raises an error if you try to commit this configuration.

SEE ALSO

What's New	 30
Known Behavior	 37
Open Issues	 38
Resolved Issues	 42
Documentation Updates	 47
Migration, Upgrade, and Downgrade Instructions	 48
Product Compatibility	 49

Known Behavior

IN THIS SECTION

- [EVPN](#) | [38](#)
- [General Routing](#) | [38](#)
- [Platform and Infrastructure](#) | [38](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the EX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- When a VLAN uses an IRB interface as the routing interface, the VLAN-ID parameter must be set to "none" to ensure proper traffic routing. This issue is platform independent. [PR1287557](#)

General Routing

- When the box is loaded and unloaded with MACsec configuration multiple times with operations made continuously, L3 connectivity is been lost and hence stops the system followed by a reboot to resume operation. [PR1416499](#)

Platform and Infrastructure

- Filters are installed only during route add if there is enough space. If the filter fails because of the non-availability of TCAM space, those routes might not be processed for filter add later when space becomes available. [PR1419926](#)

SEE ALSO

What's New	 30
What's Chnaged	 36
Open Issues	 38
Resolved Issues	 42
Documentation Updates	 47
Migration, Upgrade, and Downgrade Instructions	 48
Product Compatibility	 49

Known Issues

IN THIS SECTION

- [General Routing](#) | [39](#)
- [Infrastructure](#) | [40](#)
- [Junos Fusion Enterprise](#) | [41](#)
- [Layer 3 Features](#) | [41](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for the EX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- When a VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter will not be installed. [PR1362609](#)
- An EX4300 configured with a firewall filter on lo0 and DHCP security on a VLAN simultaneously might drop legitimate DHCP renew requests from clients on the corresponding VLANs. This occurs because of the implementation design and chipset limitation. [PR1376454](#)
- After the MACsec session is deleted, the corresponding interfaces might lose their MACsec function if LACP is enabled on them and the statement **exclude lacp** is configured under the **[edit security macsec]** hierarchy. [PR1378710](#)
- When the **show** command takes a long time to display results, the STP might change its status as BPDUs are no longer processed and cause lots of outages. [PR1390330](#)
- DCPFE did not come up in some instances of abrupt power-off/power-on of EX4650. Power-cycle of the device or host reboot will recover the device. [PR1393554](#)
- If PTP transparent clock is configured on the EX4600, and if **IGMP snooping** is configured for the same VLAN as PTP traffic, the PTP over Ethernet traffic might be dropped. [PR1395186](#)
- On EX4300 and EX4600 platforms with **flexible-ethernet-services** enabled, when **family inet/inet6** and **vlan-bridge** are configured on the same physical interface, and **family inet/inet6** is configured first, MAC address movement (MAC learning/deleting) might not happen on this interface resulting in traffic drop. [PR1408230](#)
- There is a possibility of seeing multiple reconnect logs, **JTASK_IO_CONNECT_FAILED** message during the device initialization. There is no functionality impact because of these messages. These messages can be ignored. [PR1408995](#)
- On EX9200 devices with MCLAG configuration and other features enabled, there is a loss of approximately 20 seconds during restart of the routing daemon. This traffic loss varies with the configuration that is done. [PR1409773](#)
- On EX4650 line of switches, uRPF check in strict mode might not work properly. [PR1417546](#)

- The factory-default configuration for EX4300, EX2300, EX3400, and EX4300-48MP platforms now include DHCP client configuration on IRB and VME to facilitate connectivity to phone-home server (redirect.juniper.net) from the phone-home-client running on the device. Following are the factory-default configurations:
 - DHCP enabled on VME and IRB
 - default VLAN with VLAN ID 1 and L3 interface as IRB.0 [PR1423015](#)
- On EX2300, EX3400, EX4300, and EX4600, if **igmp-snooping** is enabled, multicast traffic might be dropped silently. [PR1423556](#)
- The issue is limited to DB related to MAC move scenario. When **dhcp-security** is configured, if multiple IPv4 and IPv6 clients' MAC move occurs, the jdhcpd might consume 100 percent CPU and jdhcpd might crash. [PR1425206](#)
- Multiple EX Series platforms might be unable to commit baseline configuration after zeroization.


```
{master:0}[edit] root# commit check Mar 26 05:50:48 mustd: UI_FILE_OPERATION_FAILED: File /var/run/db/enable-process.data doesn't exist Mar 26 05:50:48 mgd[1938]: UI_FILE_OPERATION_FAILED: Failed to open /var/run/db/enable-process.data+ file error: Failed to open /var/run/db/enable-process.data+ file error: configuration check-out failed: daemon file propagation failed. PR1426341
```
- In certain scenarios, IGMP transit query packets might not be flooded on the VLAN, causing momentary drop in Layer 2 multicast traffic. [PR1427542](#)
- In case the port connecting the server from client is a trunk port and has multiple VLANs configured, then for VLAN on which NDI is not configured, the client remains in the solicit state on starting dhcpv6 device. [PR1428769](#)
- When the native VLAN is configured along with the flexible VLAN tagging on a L3 subinterface, untagged packets might be dropped on that L3 subinterface. [PR1434646](#)
- Added support for i40e NVM upgrade in EX9208. [PR1436223](#)
- NDI cannot be used in VLAN with IRB on EX92XX. Neighborhood advertisements solicit packets destined to host are getting dropped with NDI inspection (under DHCPv6 security) on a VLAN with IRB configuration on EX92XX in Junos OS Release 18.4 and later. [PR1439844](#)

Infrastructure

- On EX3400 and EX2300 line of switches during ZTP with configuration and image upgrade with FTP as file transfer, image upgrade is successful but sometimes VM core file might be generated. [PR1377721](#)
- On EX2300, EX2300-C, and EX2300-MP platforms, if Junos OS is with FreeBSD kernel version 11 with the build date on or after 2019-02-12, the switch might stop forwarding traffic or responding to console. A reboot is required to restore the service. [PR1442376](#)

Junos Fusion Enterprise

- On EX4300, when 10-Gigabit fiber port is using 1-Gigabit Ethernet SFP optics and auto-negotiation is enabled by default, the link state goes down and does not come up. [PR1420343](#)
- In a Junos Fusion Enterprise environment with EX2300-48P or EX2300-48T acting as satellite devices, loop-detect feature does not work for ports 0-23, because the loop detect filter is not properly applied. [PR1426757](#)

Layer 3 Features

- From the code analysis, the CPU rate limiting and corresponding queue points to 100 pps in Junos OS Release 12.3 for ARP traffic. But in the case of Junos OS Release 11.4, the rate limiter value is 3 Kpps. [PR1165757](#)

Platform and Infrastructure

- There are multiple failures when an event such as node reboot, ICL flap or ICCP flap occurs; and even with **enhanced convergence** configured there is no guarantee that subsecond convergence will be achieved. [PR1371493](#)
- ICMPv6 packets are hitting the dynamic ingress filter with higher priority, thus never reaching an MF or static classifier. [PR1388324](#)
- Adding the second IRB to an aggregated Ethernet and then removing it might cause the first IRB to stop working. [PR1423106](#)

Spanning Tree Protocols

- On committing **interface-range** configuration defined over wild-card range like ge-*/*/ is not supported. As a result, exceeding valid range for stp-port-ids. The commit fails. Sample example configuration is **set interfaces interface-range RANGE1 member ge-*/*/** and **set interfaces interface-range RANGE1 mtu 2000**. [PR1421446](#)
- After converging VSTP, if there is a VSTP configuration change and then BPDU might not be flooded because of which port role might be in incorrect state in the adjacent switches. There is no loop created in the network. [PR1443489](#)

SEE ALSO

[What's New | 30](#)

[What's Chnaged | 36](#)

Known Behavior 37
Resolved Issues 42
Documentation Updates 47
Migration, Upgrade, and Downgrade Instructions 48
Product Compatibility 49

Resolved Issues

IN THIS SECTION

- Authentication and Access Control | 43
- EVPN | 43
- General Routing | 43
- Infrastructure | 44
- Interfaces and Chassis | 44
- Layer 2 Ethernet Services | 45
- Junos Fusion Enterprise | 45
- Network Management and Monitoring | 45
- Platform and Infrastructure | 45
- Routing Protocols | 46
- Software Installation and Upgrade | 46
- Subscriber Access Management | 46

This section lists the issues fixed in Junos OS Release 19.2R1 for the EX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Authentication and Access Control

- Without configuring anything related to dot1x, the syslog **dot1xd[2192]: task_connect: task PNACAUTH./var/run/authd_control addr /var/run/authd_control: Connection refused** is generated repeatedly. [PR1406965](#)

EVPN

- The device might proxy the ARP probe packets in an EVPN environment. [PR1427109](#)
- ESI is configured on a single-homed 25G port might not work. [PR1438227](#)

General Routing

- On EX4650 switches, convergence delay between PE1 and P router link is more than the expected delay value. [PR1364244](#)
- OAM Ethernet **connectivity-fault-management** configured on aggregated Ethernet interfaces is not supported and no commit error is seen. [PR1367588](#)
- IPv6 router advertisement (RA) messages potentially increase internal kernel memory usage. [PR1369638](#)
- RIPv2 update packets might not be sent with IGMP snooping enabled. [PR1375332](#)
- Input rate PPS does not increase on EX2300-MP uplink ports when the packet is a pure L2 packet like non-etherII or non-EtherSnap. [PR1389908](#)
- EX3400VC - When an interface in a Virtual Chassis member switch that is not master, is flapped, IGMP query packets 224.0.0.1 are sent to all the ports of the members except the master FPC. [PR1393405](#)
- PTP over Ethernet traffic might be dropped when IGMP and PTP TC are configured together. [PR1395186](#)
- EX3400 might not learn 30,000 MAC addresses while sending MAC learning traffic. [PR1399575](#)
- MAC-limit with persistent MAC is not working after reboot. [PR1400507](#)
- After upgrading to Junos OS Release 18.1R3.3, **adt7470_set_pwm** output message is observed continuously. [PR1401709](#)
- The DHCP discover packets are forwarded out of an interface incorrectly when DHCP snooping is configured on that interface. [PR1403528](#)
- On EX4300-48MP devices, the packets drop when the traffic filter and the routing instance are configured. [PR1407424](#)
- The l2cpd might crash if the **vstp traceoptions** and **vstp vlan all** commands are configured. [PR1407469](#)
- MAC address movement might not happen in flexible Ethernet services mode when family inet/inet6 and vlan-bridge are configured on the same physical interface. [PR1408230](#)
- EX3400 PSU status is still taking "check" status even though PSU module has been removed. [PR1408675](#)

- On EX2300-24P switches, error message **dc-pfe: BCM_NH-,bcm_nh_resolve_get_nexthop(),346:Failed to find if family** is seen. [PR1410717](#)
- On EX Series devices, the PEM alarm for backup FPC remains on master FPC though the backup FPC is detached from Virtual Chassis. [PR1412429](#)
- On EX4300-48MP devices, the chassis status LED shows yellow instead of amber. [PR1413194](#)
- The chassisd output power budget is received continually per 5 seconds without any alarm after an upgrade to Junos OS Release 18.1R3. [PR1414267](#)
- VXLAN encapsulation next hop (VENH) does not get installed during BGP flap or when routing is restarted. [PR1415450](#)
- On EX3400 switches, the **show chassis environment** repeats **OK** and **Failed** at short intervals. [PR1417839](#)
- The EX3400 VC status might be unstable during the boot-up of the Virtual Chassis or after the Virtual Chassis port flaps. [PR1418490](#)
- Virtual Chassis might become unstable and FXPC crashes and generates a core file when there are a lot of configured filter entries. [PR1422132](#)
- On EX3400 auto-negotiation status shows incomplete on ge-0/2/0 using SFP-SX. [PR1423469](#)
- On EX4600 line of switches, MACsec might not connect when the interface disconnects while traffic is passing. [PR1423597](#)
- I2C read errors are seen when an SFP-T is inserted into a disabled state port configured with **set interface <*> disable** command. [PR1423858](#)
- Incorrect model information while polling through SNMP from Virtual Chassis. [PR1431135](#)

Infrastructure

- IfSpeed and IfHighSpeed erroneously reported as zero on EX2300. [PR1326902](#)
- Packet Forwarding Engine is flooded with messages **// pkt rx** on physical interface NULL unit 0. [PR1381151](#)

Interfaces and Chassis

- Missing mandatory ICCP configuration statement **redundancy-group-id-list** produces misleading error message. [PR1402606](#)
- EVPN aggregated Ethernet interface flaps followed by a commit. [PR1425339](#)

Layer 2 Ethernet Services

- The malfunction of core isolation feature in EVPN VXLAN scenarios might cause traffic to get silently dropped and discarded. [PR1417729](#)

Junos Fusion Enterprise

- PoE over LLDP negotiation is not supported on Junos Fusion Enterprise setup. [PR1366106](#)
- New satellite device cannot be added to the Fusion scenario. [PR1374982](#)
- Cascade port might go down after SD reboot in Junos Fusion Enterprise environment. [PR1382091](#)
- Cannot log in to SD cluster though it is recognized by AD properly. [PR1395570](#)
- The l2ald might crash when **clear ethernet-switching table persistent-learning** command is issued. [PR1409403](#)
- Extended ports in Junos Fusion Enterprise do not adjust MTU when VoIP is enabled. [PR1411179](#)
- The traffic might silently drop and get discarded in Junos Fusion Enterprise scenario with dual-AD. [PR1417139](#)

Network Management and Monitoring

- Over temperature trap is not sent out even when there is a temperature-hot-alarm. [PR1412161](#)

Platform and Infrastructure

- Ping does not go through the device after WTR timer expires in Ethernet ring protection switching (ERPS) scenario. [PR1132770](#)
- EX4300 upgrade fails during validation of SLAX script. [PR1376750](#)
- Unicast DHCP request gets misforwarded to backup RTG link on EX4300 Virtual Chassis. [PR1388211](#)
- EX4300 OAM LFM might not work on extended-vlan-bridge interface with **native vlan** configured. [PR1399864](#)
- Traffic drop is seen on EX4300 when 10-Gigabit fiber port is using 1-Gigabit Ethernet SFP optics with auto-negotiation enabled. [PR1405168](#)
- On EX4300, when power supply (PEM) is removed, alarm is not generated. [PR1405262](#)
- The policer might not work when it is applied through the dynamic filter. [PR1410973](#)
- The traffic to the NLB server might not be forwarded if the NLB cluster works on multicast mode. [PR1411549](#)
- EX4300 QinQ - untagged UNI traffic egress as single-tagged on NNI interface. [PR1413700](#)

- Runt counter never incremented. [PR1419724](#)
- EX4300 does not send fragmentation needed message when MTU is exceeded with DF bit set. [PR1419893](#)
- The pfex process might crash and core files might be generated when SFP is reinserted. [PR1421257](#)
- Traffic might get silently dropped when one of logical interfaces on LAG is deactivated or deleted. [PR1422920](#)
- Auditd crashes when accounting RADIUS server is not reachable. [PR1424030](#)
- The native VLAN ID of packets might fail when leaving out. [PR1424174](#)
- Interface flapping scenario might lead to ECMP next-hop install failure on EX4300 switches. [PR1426760](#)
- VIP might not forward the traffic if VRRP is configured on an aggregated Ethernet interface. [PR1428124](#)
- EX4300 does not drop FCS frames on XE interfaces. [PR1429865](#)
- The ERPS failover does not work as expected on EX4300 device. [PR1432397](#)

Routing Protocols

- Host-destined packets with filter log action might reach the Routing Engine. [PR1379718](#)
- The rpd crashes on static route configuration for multicast source. [PR1408443](#)
- Host-generated ICMPv6 RA packets might be dropped on the backup member of Virtual Chassis if **igmp-snooping** is configured. [PR1413543](#)
- The EX Series switches might not install all IRB MAC addresses in the initialization. [PR1416025](#)
- After restarting multicast-snooping process, **igmp-snooping** might not work. [PR1420921](#)

Software Installation and Upgrade

- Configuration loss and traffic loss might be seen if backup Routing Engine is zeroized and is then switched over to master within a short time. [PR1389268](#)

Subscriber Access Management

- authd reuses address quickly before jdncpd completely cleans up the old subscriber that gives the following error log **DH_SVC_DUPLICATE_IPADDR_ERR: Failed to add x.x.x.x as it is already used by xxx.** [PR1402653](#)
- On EX4300 /var showing full /var/log/dfcd_enc file grows in size. [PR1425000](#)

SEE ALSO

What's New	 30
What's Chnaged	 36
Known Behavior	 37
Open Issues	 38
Documentation Updates	 47
Migration, Upgrade, and Downgrade Instructions	 48
Product Compatibility	 49

Documentation Updates

IN THIS SECTION

- [Installation and Upgrade](#) | 47

This section lists the errata and changes in Junos OS Release 19.2R1 for the EX Series switches documentation.

Installation and Upgrade

- **Veriexec explained (EX Series)**—Verified Exec (also known as veriexec) is a file-signing and verification scheme that protects the Junos operating system (OS) against unauthorized software and activity that might compromise the integrity of your device. Originally developed for the NetBSD OS, veriexec was adapted for Junos OS and enabled by default from Junos OS Release 7.5 onwards.

[See [Veriexec Overview](#).]

SEE ALSO

What's New	 30
What's Chnaged	 36
Known Behavior	 37
Open Issues	 38

[Resolved Issues | 42](#)

[Migration, Upgrade, and Downgrade Instructions | 48](#)

[Product Compatibility | 49](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 48](#)

This section contains the upgrade and downgrade support policy for Junos OS for the EX Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network. For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://support.juniper.net/support/eol/software/junos/>.

SEE ALSO

[What's New | 30](#)

What's Chnaged 36
Known Behavior 37
Open Issues 38
Resolved Issues 42
Documentation Updates 47
Product Compatibility 49

Product Compatibility

IN THIS SECTION

- Hardware Compatibility | 49

Hardware Compatibility

To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on EX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

What's New 30
What's Chnaged 36
Known Behavior 37
Open Issues 38
Resolved Issues 42

Junos OS Release Notes for Junos Fusion Enterprise

IN THIS SECTION

- New and Changed Features | 50
- Changes in Behavior and Syntax | 51
- Known Behavior | 52
- Known Issues | 52
- Resolved Issues | 53
- Documentation Updates | 54
- Migration, Upgrade, and Downgrade Instructions | 55
- Product Compatibility | 60

These release notes accompany Junos OS Release 19.2R1 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

NOTE: For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices can function as satellite devices, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

There are no new features or enhancements to existing features in Junos OS Release 19.2R1 for Junos Fusion Enterprise.

NOTE: For more information about the Junos Fusion Enterprise features, see the [Junos Fusion Enterprise User Guide](#).

SEE ALSO

Changes in Behavior and Syntax	51
Known Behavior	52
Known Issues	52
Resolved Issues	53
Documentation Updates	54
Migration, Upgrade, and Downgrade Instructions	55
Product Compatibility	60

Changes in Behavior and Syntax

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for Junos Fusion Enterprise.

SEE ALSO

New and Changed Features	50
Known Behavior	52
Known Issues	52
Resolved Issues	53
Documentation Updates	54
Migration, Upgrade, and Downgrade Instructions	55
Product Compatibility	60

Known Behavior

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for Junos Fusion Enterprise.

For the most complete and latest information about known Junos OS problems, use the Juniper Networks online [Junos Problem Report Search](#) application.

SEE ALSO

New and Changed Features 50
Changes in Behavior and Syntax 51
Known Issues 52
Resolved Issues 53
Documentation Updates 54
Migration, Upgrade, and Downgrade Instructions 55
Product Compatibility 60

Known Issues

IN THIS SECTION

- [Junos Fusion Enterprise | 52](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for Junos Fusion Enterprise.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Junos Fusion Enterprise

- On EX4300 when 10G fiber port is using 1G Ethernet SFP optics, auto-negotiation is enabled by default. To bring up the satellite device, BCM recommends to disable the auto-negotiation for PHY84756 ports. [PR1420343](#)

- In Junos Fusion Enterprise environment with EX2300-48P or EX2300-48T acting as satellite devices, loop-detect feature does not work for ports 0-23, since the loop detect filter is not properly applied. [PR1426757](#)

SEE ALSO

New and Changed Features	 50
Changes in Behavior and Syntax	 51
Known Behavior	 52
Resolved Issues	 53
Documentation Updates	 54
Migration, Upgrade, and Downgrade Instructions	 55
Product Compatibility	 60

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 19.2R1](#) | [53](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Resolved Issues: 19.2R1

- PoE over LLDP negotiation is not supported on Junos Fusion Enterprise setup. [PR1366106](#)
- New satellite device cannot be added to the Fusion scenario. [PR1374982](#)
- Cascade port might go down after SD reboot in Junos Fusion Enterprise environment. [PR1382091](#)
- Cannot login to SD cluster though it is recognized by AD properly. [PR1395570](#)
- The l2ald might crash when **clear ethernet-switching table persistent-learning** command is issued. [PR1409403](#)

- Extended ports in JFE do not adjust MTU when VoIP is enabled. [PR1411179](#)
- The traffic might silently drop and get discarded in Junos Fusion Enterprise scenario with dual-AD. [PR1417139](#)

SEE ALSO

New and Changed Features	 50
Changes in Behavior and Syntax	 51
Known Behavior	 52
Known Issues	 52
Documentation Updates	 54
Migration, Upgrade, and Downgrade Instructions	 55
Product Compatibility	 60

Documentation Updates

There are no errata or changes in Junos OS Release 19.2R1 for documentation for Junos Fusion Enterprise.

SEE ALSO

New and Changed Features	 50
Changes in Behavior and Syntax	 51
Known Behavior	 52
Known Issues	 52
Resolved Issues	 53
Migration, Upgrade, and Downgrade Instructions	 55
Product Compatibility	 60

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading Junos OS on an Aggregation Device | 55
- Upgrading an Aggregation Device with Redundant Routing Engines | 57
- Preparing the Switch for Satellite Device Conversion | 57
- Converting a Satellite Device to a Standalone Switch | 59
- Upgrade and Downgrade Support Policy for Junos OS Releases | 59
- Downgrading from Junos OS | 59

This section contains the procedure to upgrade or downgrade Junos OS and satellite software for a Junos Fusion Enterprise. Upgrading or downgrading Junos OS and satellite software might take several hours, depending on the size and configuration of the Junos Fusion Enterprise topology.

Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the **junos-install** package. Use other packages (such as the **jbundle** package) only when so instructed by a Juniper Networks support representative. For information about the contents of the **junos-install** package and details of the installation process, see the [Installation and Upgrade Guide](#).

NOTE: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

```
user@host> request system snapshot
```

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the **juniper.conf** and **ssh** files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the [Junos OS Administration Library](#).

To download and install Junos OS:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list on the right of the page.
5. Select the **Software** tab.
6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **junos-install** package on the aggregation device.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

Customers in the United States and Canada, use the following commands:

```
user@host> request system software add validate reboot source/package-name.tgz
```

All other customers, use the following commands, where *n* is the spin number.

```
user@host> request system software add validate reboot source/package-name-limited.tgz
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:

- `ftp://hostname/pathname`
- `http://hostname/pathname`
- `scp://hostname/pathname` (available only for Canada and U.S. version)

The **validate** option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Adding the **reboot** command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to minimize disrupting network operations as follows:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos Fusion Enterprise. See [Configuring or Expanding a Junos Fusion Enterprise](#).

For satellite device hardware and software requirements, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).

Use the following command to install Junos OS on a switch before converting it into a satellite device:

```
user@host> request system software add validate reboot source/package-name
```

NOTE: The following conditions must be met before a Junos switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch running Junos OS can be converted only to SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the **request system zeroize** command, or the following command must be included in the configuration: **set chassis auto-satellite-conversion**.

When the interim installation has completed and the switch is running a version of Junos OS that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos Fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, or preconfiguration. See [Configuring or Expanding a Junos Fusion Enterprise](#) for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos Fusion topology. For more information, see [Converting a Satellite Device to a Standalone Device](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>

Downgrading from Junos OS

Junos Fusion Enterprise is first supported in Junos OS Release 16.1, although you can downgrade a standalone EX9200 switch to earlier Junos OS releases.

NOTE: You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

To downgrade a Junos Fusion Enterprise from Junos OS Release 19.2R1, follow the procedure for upgrading, but replace the 19.2 **junos-install** package with one that corresponds to the appropriate release.

SEE ALSO

[New and Changed Features | 50](#)

[Changes in Behavior and Syntax | 51](#)

[Known Behavior | 52](#)

[Known Issues | 52](#)

[Resolved Issues | 53](#)

[Documentation Updates | 54](#)

[Product Compatibility | 60](#)

Product Compatibility

IN THIS SECTION

● [Hardware and Software Compatibility | 60](#)

● [Hardware Compatibility Tool | 60](#)

Hardware and Software Compatibility

For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices function as satellite devices, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#) in the [Junos Fusion Enterprise User Guide](#).

To determine the features supported in a Junos Fusion, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

New and Changed Features	50
Changes in Behavior and Syntax	51
Known Behavior	52
Known Issues	52
Resolved Issues	53
Documentation Updates	54
Migration, Upgrade, and Downgrade Instructions	55

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

●	New and Changed Features	62
●	Changes in Behavior and Syntax	62
●	Known Behavior	63
●	Known Issues	63
●	Resolved Issues	64
●	Documentation Updates	65
●	Migration, Upgrade, and Downgrade Instructions	66
●	Product Compatibility	74

These release notes accompany Junos OS Release 19.2R1 for the Junos Fusion Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [Spanning-Tree Protocols | 62](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for Junos Fusion Provider Edge.

Spanning-Tree Protocols

- **Support for Multiple Spanning Tree Protocol (MSTP) (Junos Provider Edge)**—Starting with Junos OS Release 19.2R1, you can configure MSTP on MX480 devices. MSTP scales better than other types of spanning-tree protocols and enables load balancing.

[See [Configuring MSTP Protocol](#).]

SEE ALSO

What's Changed 62
Known Limitations 63
Open Issues 63
Resolved Issues 64
Documentation Updates 65
Migration, Upgrade, and Downgrade Instructions 66
Product Compatibility 74

Changes in Behavior and Syntax

There are no changes in the behavior of Junos OS features or in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for Junos Fusion Provider Edge.

SEE ALSO

What's New	62
Known Limitations	63
Open Issues	63
Resolved Issues	64
Documentation Updates	65
Migration, Upgrade, and Downgrade Instructions	66
Product Compatibility	74

Known Behavior

There are no known behaviors, system maximums, or limitations in hardware and software in Junos OS Release 19.2R1 for Junos Fusion Provider Edge.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

SEE ALSO

What's New	62
What's Changed	62
Open Issues	63
Resolved Issues	64
Documentation Updates	65
Migration, Upgrade, and Downgrade Instructions	66
Product Compatibility	74

Known Issues

IN THIS SECTION

- [Junos Fusion Provider Edge](#) | [64](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for Junos Fusion Provider Edge.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Junos Fusion Provider Edge

- If a default shaper is applied to a cascade interface of an aggregation device (AD), the displayed value of "Guaranteed rate" is greater than the value of "Shaping rate" in the output of the **show class-of-service scheduler-hierarchy interface** command. [PR1415502](#)

SEE ALSO

What's New 62
What's Changed 62
Known Limitations 63
Resolved Issues 64
Documentation Updates 65
Migration, Upgrade, and Downgrade Instructions 66
Product Compatibility 74

Resolved Issues

IN THIS SECTION

- [Junos Fusion Provider Edge | 65](#)
- [Junos Fusion Satellite Software | 65](#)

This section lists the issues fixed in Junos OS Release 19.2R1 for Junos Fusion Provider Edge.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Junos Fusion Provider Edge

- Auto-negotiation is not disabled in the hardware after the no-auto-negotiation option is set using the CLI. [PR1411852](#)

Junos Fusion Satellite Software

- Extended Port (EP) LAG might go down on the Satellite Devices (SDs) if the related Cascade Port (CP) links to an Aggregation Device (AD) goes down. [PR1397992](#)

SEE ALSO

What's New 62
What's Changed 62
Known Limitations 63
Open Issues 63
Documentation Updates 65
Migration, Upgrade, and Downgrade Instructions 66
Product Compatibility 74

Documentation Updates

There are no errata or changes in Junos OS Release 19.2R1 documentation for Junos Fusion Provider Edge.

SEE ALSO

What's New 62
What's Changed 62
Known Limitations 63
Open Issues 63
Resolved Issues 64
Migration, Upgrade, and Downgrade Instructions 66
Product Compatibility 74

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Basic Procedure for Upgrading an Aggregation Device | 66
- Upgrading an Aggregation Device with Redundant Routing Engines | 69
- Preparing the Switch for Satellite Device Conversion | 69
- Converting a Satellite Device to a Standalone Device | 71
- Upgrading an Aggregation Device | 73
- Upgrade and Downgrade Support Policy for Junos OS Releases | 73
- Downgrading from Junos OS Release 19.2 | 74

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos Fusion Provider Edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

When upgrading or downgrading Junos OS, always use the **jinstall** package. Use other packages (such as the **jbundle** package) only when so instructed by a Juniper Networks support representative. For information about the contents of the **jinstall** package and details of the installation process, see the [Installation and Upgrade Guide](#).

NOTE: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

```
user@host> request system snapshot
```

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the **juniper.conf** and **ssh** files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the [Installation and Upgrade Guide](#).

The download and installation process for Junos OS Release 19.2R1 is different from that for earlier Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the page.
5. Select the **Software** tab.
6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the aggregation device.

NOTE: We recommend that you upgrade all software packages out-of-band using the console, because in-band connections are lost during the upgrade process.

Customers in the United States and Canada, use the following commands.

- For 64-bit software:

NOTE: We recommend that you use 64-bit Junos OS software when implementing Junos Fusion Provider Edge.

```
user@host> request system software add validate reboot  
source/jinstall64-19.2R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-19.2R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

NOTE: We recommend that you use 64-bit Junos OS software when implementing Junos Fusion Provider Edge.

```
user@host> request system software add validate reboot
source/jinstall64-19.2R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-19.2R1.SPIN-export-signed.tgz
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
 - **ftp://hostname/pathname**
 - **http://hostname/pathname**
 - **scp://hostname/pathname** (available only for the Canada and U.S. version)

The **validate** option validates the software package against the current configuration as a prerequisite for adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is for a different release.

Adding the **reboot** command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 19.2R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately as follows to minimize disrupting network operations:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos Fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. For satellite device hardware and software requirements, see [Understanding Junos Fusion Software and Hardware Requirements](#)

NOTE: The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch can be converted to only SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the **request system zeroize** command, or the following command must be included in the configuration: **set chassis auto-satellite-conversion**.

Customers with EX4300 switches, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-ex-4300-14.1X53-D43.3-domestic-signed.tgz
```

Customers with QFX5100 switches, use the following command:

```
user@host> request system software add reboot
source/jinstall-qfx-5-14.1X53-D43.3-domestic-signed.tgz
```

When the interim installation has completed and the switch is running a version of Junos and OS on one line that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device by using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device by using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose your connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```


This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos Fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See [Configuring Junos Fusion Provider Edge](#) for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos Fusion topology.

NOTE: If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is software that includes *pxe* in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named `install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz`. If the satellite device is an EX4300 switch, you install a standard `jinstall-ex-4300` version of Junos OS.

The following steps explain how to download software, remove the satellite device from Junos Fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads>
2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos Fusion** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the Junos OS Release 14.1X53-D30 software image for your platform.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the routing platform or to your internal software distribution site.

8. Remove the satellite device from the automatic satellite conversion configuration.

If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID.

```
[edit]
user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
satellite member-number
```

For example, to remove member number 101 from Junos Fusion:

```
[edit]
user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
satellite 101
```

You can check the automatic satellite conversion configuration by entering the **show** command at the **[edit chassis satellite-management auto-satellite-conversion]** hierarchy level.

9. Commit the configuration.

To commit the configuration to both Routing Engines:

```
[edit]
user@aggregation-device# commit synchronize
```

Otherwise, commit the configuration to a single Routing Engine:

```
[edit]
user@aggregation-device# commit
```

10. Install the Junos OS software on the satellite device to convert the device to a standalone device.

```
[edit]
user@aggregation-device> request chassis satellite install URL-to-software-package fpc-slot
member-number
```

For example, to install a PXE software package stored in the **/var/tmp** directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install
/var/tmp/install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz fpc-slot 101
```

For example, to install a software package stored in the **var/tmp** directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

```
[edit]
```

```
user@aggregation-device> request chassis satellite install  
/var/tmp/jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz fpc-slot 101
```

The satellite device stops participating in the Junos Fusion topology after the software installation starts. The software upgrade starts after this command is entered.

11. Wait for the reboot that accompanies the software installation to complete.
12. When you are prompted to log back into your device, uncable the device from the Junos Fusion topology. See *Removing a Transceiver from a QFX Series Device* or *Remove a Transceiver*, as needed. Your device has been removed from Junos Fusion.

NOTE: The device uses a factory-default configuration after the Junos OS installation is complete.

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 19.2R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.


You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

Downgrading from Junos OS Release 19.2

To downgrade from Release 19.2 to another supported release, follow the procedure for upgrading, but replace the 19.2 **jinstall** package with one that corresponds to the appropriate release.

 **NOTE:** You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

SEE ALSO

What's New	 62
What's Changed	 62
Known Limitations	 63
Open Issues	 63
Resolved Issues	 64
Documentation Updates	 65
Product Compatibility	 74

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility](#) | 74

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on MX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature

information to find the right software release and hardware platform for your network. See the [Feature Explorer](#).

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

[What's New | 62](#)

[What's Changed | 62](#)

[Known Limitations | 63](#)

[Open Issues | 63](#)

[Resolved Issues | 64](#)

[Documentation Updates | 65](#)

[Migration, Upgrade, and Downgrade Instructions | 66](#)

Junos OS Release Notes for MX Series 5G Universal Routing Platform

IN THIS SECTION

- [New and Changed Features | 76](#)
- [Changes in Behavior and Syntax | 96](#)
- [Known Behavior | 100](#)
- [Known Issues | 102](#)
- [Resolved Issues | 111](#)
- [Documentation Updates | 129](#)
- [Migration, Upgrade, and Downgrade Instructions | 130](#)
- [Product Compatibility | 137](#)

These release notes accompany Junos OS Release 19.2R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [New and Changed Features: 19.2R1-S4 | 77](#)
- [New and Changed Features: 19.2R1-S1 | 77](#)
- [New and Changed Features: 19.2R1 | 78](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for the MX Series routers.

New and Changed Features: 19.2R1-S4

Interfaces and Chassis

- **Support for 1-Gbps on QFX-60S line card on PTX10008 and PTX10016 Routers**—QFX10000-60S-6Q line card supports 1-Gbps speed on its ports (0 to 59). The QFX10000-60S-6Q line card contains 60 SFP+ ports that support 10-Gbps, two dual-speed QSFP28 ports that support either 40-Gbps or 100-Gbps, and four QSFP+ ports that support 40-Gbps. You can individually configure ports 0 to 59 for 10-Gbps or 1-Gbps port speed. Use the **set chassis fpc fpc-slot-number pic pic-number port port-number speed 1G** command to change the mode of a port from 10-Gbps to 1-Gbps. The transceivers supported for 1-Gbps are QFX-SFP-1GE-LX, QFX-SFP-1GE-SX, and QFX-SFP-1GE-T.

[See [QFX10000 Line Cards](#) for details on the combination of modes supported on the ports.]

Services Applications

- **Support for Two-Way Active Measurement Protocol (TWAMP) and hardware timestamping of RPM probe messages (MX10000 and PTX10000 routers)**—Starting in Release 19.2R1-S4, Junos OS supports TWAMP and hardware timestamping of RPM probe messages on the MX10008, MX10016, PTX10008 and PTX10016 routers. You can use TWAMP to measure IP performance between two devices in a network. By enabling hardware timestamping of RPM you can account for the latency in the communication of probe messages and also generate more accurate timers in the Packet Forwarding Engine.

[See [Understanding Two-Way Active Measurement Protocol on Routers](#) and [Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX and MX Series Routers](#).]

New and Changed Features: 19.2R1-S1

MPLS

- **Distributed CSPF for segment routing LSPs (MX Series)**—Starting in Junos OS Release 19.2R1-S1, you can compute a segment routing LSP locally on the ingress device according to the constraints you have configured. With this feature, the LSPs are optimized based on the configured constraints and metric type. The LSPs are computed to utilize the available ECMP paths to the destination.

Prior to Junos OS Release 19.2R1-S1, for traffic engineering of segment routing paths, you could either explicitly configure static paths, or use computed paths from an external controller.

[See [Enabling Distributed CSPF for Segment Routing LSPs](#).]

- **Color-based mapping of VPN services over SRTE (MX Series)**—Starting in Junos OS Release 19.2R1-S1, you can specify a color attribute along with an IP protocol next hop to resolve transport tunnels over static colored and BGP segment routing traffic-engineered (SRTE) label-switched paths (LSPs). This is called the color-IP protocol next hop resolution, where you are required to configure a resolution-map and apply it to the VPN services. Prior to this release, the VPN services were resolved over IP protocol next hops only.

With this feature, you can enable color-based traffic steering of Layer 2 and Layer 3 VPN services.

[See [Color-Based Mapping of VPN Services Overview](#).]

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Hardware

- **New fixed-configuration Modular Port Concentrator (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.2R1, the MPC10E-10C-MRATE is a new Modular Port Concentrator (MPC) that is supported on the MX240, MX480, and MX960 routers.

The MPC10E-10C-MRATE features the following:

- Line-rate throughput of up to 1.0 Tbps when installed with an enhanced midplane and 800 Gbps when installed with a standard midplane.
- Eight QSFP28 ports—Port numbers 0/0 through 0/3 and 1/0 through 1/3. The ports can be configured as 10-Gbps, 40-Gbps, or 100-Gbps Ethernet ports.
- Two QSFP56-DD ports—Port numbers 0/4 and 1/4. The ports can be configured as 10-Gbps, 40-Gbps, 100-Gbps Ethernet ports.

[See [MX Series 5G Universal Routing Platform Interface Module Reference](#).]

- **MX10016 Universal Routing Platform**—The MX10016 router provides 10-Gigabit Ethernet, 40-Gigabit Ethernet, and 100-Gigabit Ethernet modular solutions that support up to 2.4 Tbps per slot. The MX10016 router provides redundancy and resiliency. All major hardware components including the power system, the cooling system, the control board and the switch fabrics are fully redundant. MX10016 enables cloud and data center operators to transition from 10-Gigabit Ethernet and 40-Gigabit Ethernet networks to 100-Gigabit Ethernet high-performance networks. The 21 rack unit (21 U) modular chassis can provide 38.4 Tbps of throughput. The MX10016 router has 16 slots for the line cards that can support a maximum of 1536 10-Gigabit Ethernet ports, 384 40-Gigabit Ethernet ports, or 384 100-Gigabit Ethernet ports.

You can deploy the MX10016 router in an IP edge network using an MX10K-LC2101 line card (ordering model number is JNP10K-LC2101).

[See [MX10016 Hardware Guide](#).]

- **Advanced Cooling and Power Components (MX10008 Routers)**—Starting in Junos OS Release 19.2R1, MX10008 routers offer 5.5 KW power supplies, new high performance fan tray, and compatible fan tray controller. The JNP10K-PWR-AC2 power supply supports AC, high-voltage alternating current (HVAC), DC, or high-voltage direct current (HVDC). The JNP10K-PWR-DC2 provides a 5.5 KW upgrade for DC users. The JNP10008-FAN2 offers increased air flow through the chassis. The JNP10008-FAN2 offers

1793 cubic feet per minute (CFM) per fan tray. The new fan tray controller, JNP10008-FTC2 supports the new fan tray.

[See [MX10008 Hardware Guide](#).]

Authentication, Authorization and Accounting (AAA) (RADIUS)

- **Option to enable and disable SCP per user level independent of SSH (MX Series)**—Starting in Junos OS 19.2R1, you can enable and disable SCP for a certain login class user independent of SSH. By default, SCP is not allowed for users added to the system defined classes read-only, operator and unauthorized and is only allowed to the system defined class super-user. SCP is allowed for any login class user belonging to a user defined class. You can deny SCP request for a user assigned to a user defined class by using the **no-scp-server** configuration statement. Prior to 19.2R1, SCP was enabled and disabled when SSH was enabled and disabled.

To disable SCP for a certain login class, use set **no-scp-server** at the **[edit system login class <class_name>]** hierarchy level.

[See [no-scp-server](#).]

- **Option to enable and disable SFTP per user level (MX Series)**—Starting in Junos OS 19.2R1, you can enable and disable SFTP for a certain login class user. By default, SFTP is not allowed for users added to the system defined classes read-only, operator and unauthorized and is only allowed to the system defined class super-user if SFTP is enabled globally. For a user assigned to a user defined class, by default SFTP requests are allowed if **set system services ssh sftp-server** is configured. You can now deny SFTP requests for a user assigned to a user defined class by using the **no-sftp-server** configuration statement.

To disable SFTP for a certain login class, use set **no-sftp-server** at the **[edit system login class <class_name>]** hierarchy level.

[See [no-sftp-server](#).]

EVPN

- **Support for BFD, BGP, IS-IS, and OSPF on IRB interfaces in EVPN-MPLS networks (MX Series and vMX)**—Starting with Junos OS Release 19.2R1, you can configure Bidirectional Forwarding Detection (BFD), BGP, IS-IS, and OSPF routing protocols on the IRB interface in an EVPN-MPLS network to route and forward EVPN traffic. This feature supports single-homed, single-active, and all-active multihomed networks.

[See [EVPN with IRB Solution Overview](#).]

- **EVPN support of VLAN ID ranges and lists in service provider style interface configurations (MX Series routers, and vMX virtual routers)**—Starting in Junos OS Release 19.2R1, EX9200 switches, ACX5448 and MX Series routers, and vMX virtual routers support the use of VLAN ID ranges and lists in a service provider style interface configuration, which must be referenced in an EVPN routing instance. This configuration is supported with the following EVPN environments, services, and features:

- Environments:
 - EVPN with VXLAN encapsulation

- EVPN with MPLS encapsulation
- VLAN bundle service:
 - E-LAN
 - E-Tree
 - E-Line
- Feature:
 - EVPN multihoming:
 - All-active
 - Single-active
 - Singlehoming

[See [VLAN ID Ranges and Lists in an EVPN Environment](#).]

- **Connectivity fault management support in EVPN-VPWS (MX Series)**—Starting with Junos OS Release 19.2R1, you can configure Up maintenance association end points (MEPs) and maintenance association intermediate point (MIPs) on attachment circuits in support of connectivity fault management (CFM) in EVPN-VPWS networks. With the MEPs, you can monitor connectivity between two points on the EVPN-VPWS network. Junos OS supports the continuity check messages (CCM), loopback and link trace messages (LTMs) as defined in IEEE 802.1AG CFM, and delay measurements (DM) and synthetic loss measurements (SLMs) as defined in Y.1731 on a single-active homing network.

[See [Connectivity Fault Management Support for EVPN and Layer 2 VPN Overview](#).]

- **Support for control word in EVPN-VPWS (MX Series and vMX)** —Starting with Junos OS Release 19.2R1, Junos OS supports the insertion of a control word between the label stack and the MPLS payload in a network with EVPN-VPWS service. This feature prevents a transit device from delivering out-of-order packets as a result of the device's load-balancing hashing algorithm. When you enable the control word feature on a PE device, the PE device advertises support for a control word. If all the PE devices in an EVI on the EVPN-VPWS serviced network support control word, then the PE device inserts a control word between the label stack and the L2 header in the packet thus preventing the packet from being misidentified by transit devices.

[See [Control Word for EVPN-VPWS](#).]

Forwarding and Sampling

- **Support for local preference when selecting forwarding next-hops for ECMP traffic (MX Series)**—Starting in Junos OS Release 19.2R1, you can have equal cost multi-path (ECMP) traffic flows prefer local forwarding next-hops over remote ones. This feature supports BGP prefixes that are directly reachable with IPv4 MPLS ECMP next-hops. Use **ecmp-local-bias** to direct ECMP traffic towards local links, for example, to ensure that the overall load on the fabric is reduced. [See [ecmp-local-bias](#) for usage details.]

High Availability (HA) and Resiliency

- **ISSU support for MX2008 (MX Series)**—Starting in Junos OS Release 19.2R1, MX2008 routers support ISSU.

[See [Understanding In-Service Software Upgrade \(ISSU\)](#)]

Interfaces and Chassis

- **Support for local preference when selecting forwarding next-hops for load balancing (MX Series)**—Starting in Junos OS Release 19.2R1, you can have traffic flows across aggregated Ethernet or logical-tunnel interfaces prefer local forwarding next-hops over remote ones, for example to ensure that the overall load on the fabric is reduced. [See [local-bias](#) for usage details.]
- **Support to collect and display PRBS statistics (MX10003 and MX204)**—Starting in Junos OS Release 19.2R1, on MX10003 and MX204 routers, you can check the physical link connectivity by issuing the **test interfaces ifd-name prbs-test-start pattern-type type direction (0|1) flip (0|1)** that starts collecting the PRBS statistics.

The output of the **show interfaces interface-name prbs-stats** command displays the PRBS statistics while the test is in progress. These statistics are cleared after the test is complete or if it is stopped. You can stop collecting the statistics by issuing the **test interfaces ifd-name prbs-test-stop direction (0|1)** command.

NOTE: While running PRBS statistics, the link will be down.

[See [prbs-test-start](#), [prbs-test-stop](#), [show interfaces prbs-stats](#), [Collecting Pseudo Random Bit Sequence \(PRBS\) Statistics](#).]

- **Domain Name System (DNS) is VRF aware (MX Series)**—Starting in Junos OS Release 19.2R1, when the **management-instance** statement is configured at the **[edit system]** hierarchy level, you can use the non-default management routing instance **mgmt_junos** as the routing instance through which the DNS name server is reachable. To specify the routing instance **mgmt_junos**, configure our new configuration statement **routing-instance mgmt_junos**, at the **[edit system name-server server-ip]** hierarchy level.

[See [Management Interface in a Nondefault Instance](#), [Configuring a DNS Name Server for Resolving a Hostname into Addresses](#), [name-server](#), and [show host](#).]

- **SCBE3-MX interoperates with MPC10E-10C (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.2R1, the Enhanced Switch Control Board SCBE3-MX (model number: SCBE3-MX-S) supports fabric management on the MPC10E-10C line card on the MX240, MX480, and MX960 routers. The

SCBE3-MX-S supports a pluggable Routing Engine and provides a control plane and data plane interconnect to each line card slot. The MPC10E-10C supports a bandwidth of up to 1 Tbps (800 Gbps with four planes and 1 Tbps with 5 or 6 planes). With MPC10E 15C line card, in a non-redundant configuration the SCBE3-MX provides fabric bandwidth of up to 1 Tbps per slot with four fabric planes and 1.5 Tbps per slot when all six fabric planes are used. Starting in this release, the MPC10E line cards support the standard midplane, which supports a bandwidth up to 800 Gbps per slot. Support for the enhanced midplane, which provides a bandwidth of 1.5 Tbps with MPC10E-15C and 1 Tbps with MPC10E-10C, is already available.

[See [SCBE3-MX Description](#) and [MPC10E-15C-MRATE](#)]

- **Support for QSFP-100GE-DWDM2 transceiver (MX204, MX10003, MX10008, and MX10016)**—Starting in Junos OS Release 19.2R1, the MX204, MX10003, MX10008, and MX10016 routers support the QSFP-100GE-DWDM2 transceiver. The 100-Gbps bidirectional transceiver has a dual transmitter/receiver that enables it to transmit and receive data through a single optical fiber. You can perform the following actions when this transceiver is installed:
 - View the diagnostics data, warnings, and alarms for interfaces. [See [show interfaces diagnostics optics](#).]
 - Clear the bit error rate (BER) counters. [See [clear interfaces statistics](#).]
 - Obtain the transport, performance monitoring, and threshold crossing alert (TCA) information for interfaces. [See [show interfaces transport pm](#).]
 - Clear the optics information from transport performance monitoring data. [See [clear interfaces transport pm](#).]
 - Enable or disable TCAs. [See [tca](#).]
 - Enable or disable loopback mode. [See [optics-options](#).]
- **MPC10 distributed LACP support in PPM AFT (MX Series)**—Starting in Junos OS Release 19.2R1, the MPC10E-15C-MRATE and MPC10E-10C-MRATE MPCs support distributed LACP in Periodic Packet Manager (ppman) Advanced Forwarding Toolkit (AFT).
- **Support for Routing Engine hard disk smart check (MX240, MX480, MX204, MX960, MX10008, MX2008, MX2020, MX10016, MX10000, MX2010, MX10002, and MX10003)**—Starting in Junos OS Release 19.2R1, you can configure the device to perform certain health checks on the Routing Engine solid-state drive (SSD) and log a health event or raise an alarm in case a predefined health attribute threshold is breached. You can use the **set chassis routing-engine disk smart-check** command to instruct the system to raise an alarm when an SSD health attribute threshold is breached. You can view the alarm by using the command **show chassis alarms**.

[See [smart-check](#)]

Junos OS XML API and Scripting

- **Automation script library additions and upgrades (MX Series)**—Starting in Junos OS Release 19.2R1, devices running Junos OS that support the Python extensions package include new and upgraded Python modules. Python automation scripts can leverage new on-box Python modules, including the **requests**, **chardet**, and **urllib3** modules, as well as upgraded versions of the **idna**, **ipaddress**, and **six** modules. The Requests library provides additional methods for supporting initial deployments as well as for performing routine monitoring and configuration changes on devices running Junos OS.

[See [Overview of Python Modules Available on Devices Running Junos OS](#) and [Using the Requests Library for Python on Devices Running Junos OS](#).]

Junos Telemetry Interface

- **Inline active flow monitoring support using JTI (MPC10E-15C-MRATE line cards)**—Starting in Junos OS Release 19.2R1, Junos Telemetry Interface (JTI) supports streaming inline active flow monitoring service-related statistics and errors counters for export to outside collectors at configurable intervals using remote procedure call (gRPC) services.

Use the following resource path to export statistics:

`/junos/system/linecard/services/inline-jflow/`

To provision the sensor to export data through gRPC services, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Configuring Flow Aggregation on MX, M, vMX and T Series Routers and NFX250 to Use Version 9 Flow Templates](#), [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Packet Forwarding Engine support for JTI (MX2010 and MX2020 routers)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) supports streaming of Packet Forwarding Engine statistics for MX2010 and MX2020 routers using Remote Procedure Calls (gRPC). gRPC is a protocol for configuration and retrieval of state information.

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **Sensor-level statistics support on JTI (MX960, MX2008, MX2010, MX2020, PTX5000, PTX1000, and PTX10000 routers and QFX5100 and QFX5200 switches)**—Starting with Junos OS Release 19.2R1, you can issue the Junos operational mode command **show network-agent statistics** to provide more information on a per-sensor level for statistics being streamed to an outside collector by means of remote procedure calls (gRPC) and Junos telemetry interface (JTI). Only sensors exported with gRPC are supported. The command does not support UDP-based sensors.

[See [show network-agent statistics](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **ONCE mode supported using gNMI services and JTI (MX Series)**—Starting in Junos OS Release 19.2R1, you can include the "ONCE" mode with the **Subscribe** RPC when subscribing to gRPC Network Management Interface (gNMI) services to export statistics for telemetry monitoring and management using Junos telemetry interface (JTI). ONCE mode ensures that the collector is only streamed telemetry information one time.

The Subscribe RPC and subscription parameters are defined in the [gnmi.proto](#) file.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Packet Forwarding Engine statistics export using gNMI and JTI (MX960, MX2008, MX2010 and MX2020 routers)**—Starting in Junos OS Release 19.2R1, you can stream Packet Forwarding Engine statistics to an outside collector using gRPC Management Interface (gNMI) version 0.7.0 and Junos telemetry interface (JTI). Prior to this, these statistics were exported using OpenConfig gRPC and UDP protocol buffer (gpb) format. OpenConfig gRPC and gNMI are both protocols used to modify and retrieve configurations as well as export telemetry streams from a device in order to manage and monitor it

To provision Packet Forwarding Engine sensors to export data through gNMI, use the Subscribe RPC defined in the [gnmi.proto](#) to specify request parameters. This RPC already supports Routing Engine statistics to be exported by means of gNMI. Now, Packet Forwarding Engine sensors will also stream KV pairs in gNMI format for a majority of Packet Forwarding Engine sensors.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Broadband edge statistics support through JTI (MX Series)**—Starting in Junos OS Release 19.2R1, subscriber-based telemetry streaming is enabled when an MX Series router is configured for Broadband Network Gateway (BNG) and Junos Fusion where subscribers are connected through Junos Fusion Satellite devices. You can use remote procedure calls (gRPC) to export broadband edge (BBE) telemetry statistics to external collectors. gRPC is a protocol for configuration and retrieval of state information.

You can stream all BBE resource paths except for the following:

- `/junos/system/subscriber-management/access-network/ancp`
- `/junos/system/subscriber-management/client-protocols/l2tp`
- `/junos/system/subscriber-management/infra/network/l2tp/`

To stream BBE statistics, include a resource path starting with `/junos/system/subscriber-management/` in your gRPC subscription.

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **gRPC-based streaming telemetry support for subscriber service accounting statistics for JTI (MX Series 5G Universal Routing Platform)**—Starting in Junos OS Release 19.2R1, you can enable service filter accounts statistics for subscribers using Junos telemetry interface (JTI) and remote procedure calls (gRPC). Service accounting statistics include IP protocol IPv4 family, IPv6 family, or both, as well as transmit and receive packets and bytes for subscriber service sessions.

To enable these statistics from an MX Series router, include the **service-statistics** statement at the **[edit dynamic-profiles my-service-profile telemetry]** hierarchy level.

To stream these statistics, include the resource path `/junos/system/subscriber-management/dynamic-profiles/interfaces/services/` in your gRPC subscription to export the statistics to an outside collector.

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) **service-statistics**, and [Enable Service Filter Accounting Statistics for Subscribers](#).]

- **FPC and optics support for JTI (MX Series)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) supports streaming of Flexible PIC Concentrator (FPC) and optics statistics for the MX Series router using remote procedure calls (gRPC). gRPC is a protocol for configuration and retrieval of state information. This feature effort includes the addition of a new process (SensorD daemon) to export telemetry data for integration with AFTTelemetry and LibTelemetry libraries in the OpenConfig model called AFT platform.

The following base resource paths are supported:

- `/junos/system/linecard/environment/`
- `/junos/system/linecard/optics/`
- `/junos/system/linecard/optics/optics-diag[if-name =]`
- `/junos/system/linecard/optics/optics-diag/if-name`

- `/junos/system/linecard/optics/optics-diag/snmp-if-index`
- `/junos/system/linecard/optics/lane[lane_number=]/`

To provision the sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. Streaming telemetry data through gRPC also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **Specify Routing Instance for JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 19.2R1, you can specify the routing instance to use for remote procedure call (gRPC) services. Include the **routing-instance** *instance-name* at the **[edit system services extension-service request-response grpc]** hierarchy level. The routing instance name specified should match the name of the existing routing instance, such as a name configured under the **[routing-instances]** hierarchy level or **mgmt_junos** if **system management-instance** is configured (the dedicated management routing instance).

Configuring the routing instance lets you choose the VRF for gRPC services. When the routing instance is not configured, the default behavior is that all gRPC-related services are available through the management **fxp0/em0** interface.

Layer 2 VPN

- **Support for group key acknowledgment messages (MX Series)**—Starting with Junos OS Release 19.2R1, Junos OS supports group members sending acknowledgment messages as defined in RFC 8263 in response to group key push messages sent by group controllers and key servers. The group member sends acknowledgment messages when it receives a group key push message with a standard KEK_ACK_REQUESTED value of 9 in the SA KEK payload as defined in RFC 8263 or a KEK_ACK_REQUESTED value of 129 that is used in older key servers. No additional configuration is required.

[See [Group VPNv2 Overview](#).]

Layer 2 Features

- **Support for basic Layer 2 features on MPC10E-15C-MRATE line card (MX Series)**—Starting in Junos OS Release 19.2R1, MPC10E-15C-MRATE line card supports the following basic Layer 2 features:
 - Layer 2 bridging with trunk and access modes
 - MAC learning and aging
 - Handling BUM (broadcast, unknown unicast and multicast) traffic, including split horizon
 - MAC move
 - Layer 2 forwarding and flooding statics
 - Mesh groups

- Static MAC addresses
- MAC learning and forwarding on AE interfaces
- Bridging on untagged interfaces
- Basic Q-n-Q tunneling (without VLAN-translation and VLAN map operations)

[See [Understanding Layer 2 Bridge Domains](#), [Understanding Layer 2 Learning and Forwarding](#).]

Layer 3 Features

- **MPC10E-10C and MPC10E-15C support layer 3 routing features (MX240, MX480, and MX960)**—Starting in Junos OS Release 19.2R1, MPC10E-10C and MPC10E-15C line cards support the following features in hyper-mode:
 - Configuring ICMP redirects and generating ICMP redirect messages.
 - Padding VLAN packets to a minimum frame size of 68 bytes, by using the existing command **set interfaces *interface-name* gigether-options pad-to-minimum-frame-size**.
 - Collecting interface family statistics for IPv4 and IPv6, by using the existing command **show interfaces statistics detail *interface-name***.

See [Understanding the Hyper Mode Feature on Enhanced MPCs for MX Series Routers and EX9200 Switches](#)

MPLS

- **Dynamic creation of segment routing LSPs using BGP protocol next hops (MX Series)**—Starting in Junos OS Release 19.2R1, you can configure tunnel templates on colored and non-colored segment routing traffic-engineered (SR-TE) paths. These templates enable dynamic creation of segment routing tunnels using protocol next hops with BGP prefixes to resolve destination segment identifiers (SIDs).

With this feature, you can benefit from reduced configuration, especially when the network deployment requires connectivity from each provider edge (PE) device to every other PE device.

[See [Static Segment Routing Label Switched Path](#).]

- **CSC support for MPLS-over-UDP tunnels (MX Series with MPC and MIC and VMX)**—Starting in Junos Release 19.2R1, carrier supporting carrier (CSC) architecture can be deployed with MPLS-over-UDP tunnels carrying MPLS traffic over dynamic IPv4 UDP tunnels that are established between supporting carrier's provider edge (PE) devices. With this enhancement, the scaling advantage that the MPLS-over-UDP tunnels provided is further increased. This feature is not supported on IPv6 UDP tunnels.

[See [Example: Configuring Next-Hop-Based MPLS-Over-UDP Dynamic Tunnels](#).]

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (MX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data

model when you include the **action-expand** extension statement in the option or statement definition and reference a script that handles the logic. The **action-expand** statement must include the **script** child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

- **Support for Synchronous Ethernet with ESMC on JNP10K-LC2101 (MX10008 and MX10016)**—Starting in Junos OS Release 19.2R1, the JNP10K-LC2101 line card supports Synchronous Ethernet (SyncE) with ESMC. Synchronous Ethernet is a physical layer technology that is used to transfer clock signals over Ethernet interfaces. ESMC transmits Synchronization Status Message (SSM) information, which is the quality level of the transmitting synchronous Ethernet equipment clock (EEC), by using ESMC protocol data units (PDUs). This support allows you to configure BITS-0 (external-0) and BITS-1 (external-1) ports as clock sources or outputs on master Routing and Control Board (JNP10K-RE1). You can also configure a GPS (external-2) port as a clock source on master Routing and Control Board. This feature also supports SyncE over aggregated Ethernet (AE).

NOTE: Only the GPS port and BITS ports that are configured on master RCB are active.

[[Centralized Clocking Overview](#) and [Understanding ESMC Quality Level Mapping](#)]

- **Support for optimizing the SNMP walk execution time for IPsec statistics (MX Series)**—Starting in Junos OS Release 19.2R1, you can optimize the SNMP walk execution time for IPsec statistics. To achieve this optimization, increase the cache lifetime of the IPsec related information (for example statistics and SA information) so that a single SNMP walk request is served for N number of IPsec Security Associations (SAs) with N number of queries made to the service PIC. IPsec statistics are now fetched by the burst mode, thereby reducing the load on the Routing Engine daemon, kmd. For different scale needs, we may have to tweak the hidden SNMP knob parameters, for example, with Dead Peer detection (DPD) having more number of tunnels without traffic and simultaneous SNMP walks.

Port Security

- **Fallback PSK for Media Access Control Security (MACsec) (MX Series)**—Starting in Junos OS Release 19.2R1, fallback PSK for MACsec is supported on MX Series routers that support MACsec. The fallback PSK provides functionality to establish a secure session in the event that the primary PSKs on each end of a MACsec-secured link do not match.

[See [Configuring Media Access Control Security \(MACsec\) on MX Series Routers](#).]

Routing Policy and Firewall Filters

- **Support for CCC and Layer 3 firewall forwarding on MPC10E-15C-MRATE line cards (MX Series)**—Starting with Junos OS Release 19.2R1, circuit cross-connect (CCC) traffic and Layer 3 firewall forwarding features are supported on MPC10E-15C-MRATE line cards.

[See [CCC Overview](#) and [Protocols and Applications Supported by the MPC10E-15C-MRATE](#).]

Routing Protocols

- **MPC10 Inline BFD support (MX Series)**—Starting in Junos OS Release 19.2, MPC10 MPCs support inline BFD features, excluding micro BFD and BFD sessions with authentication.

[See [Understanding BFD for Static Routes](#).]

- **Support for IPv6 fragment reassembly for v4ov6 dynamic tunnels**—Starting in Junos OS Release 19.1R1, you can configure an additional attribute, **dynamic-tunnel-reassembly-enable** for reassembling IPv6 fragments before the termination of v4ov6 tunnels. The fragment reassembly feature is disabled by default. IPv6 fragments are discarded when this feature is not enabled.
- **IPv6 reassembly for v4ov6 tunnels (MX Series)**—Starting in Junos OS 19.2R1, you can enable the MX chassis to perform IPV6 fragment reassembly for forwarding Ipv4 traffic. When the **dynamic-tunnel-reassembly** is configured, the tunnels using the attribute would be setup for reassembling the IPv6 fragments before the termination of v4ov6 tunnels. By default, this attribute is turned off and the tunnels are set up to discard the IPv6 fragments.

To enable IPv6 fragment reassembly for forwarding Ipv4 traffic, use **set dynamic-tunnel-reassembly on** statement at the **[edit routing-options dynamic-tunnels tunnel-attributes <dynamic-tunnel-name>]** hierarchy level.

[See [dynamic-tunnel-reassembly](#).]

- **Map single IPv6 anycast address on multiple anchor Packet Forwarding Engines (MX240, MX480, MX960, MX2020)**—Starting in Junos OS Release 19.2R1, you can assign the same IPv6 anycast address to multiple anchor Packet Forwarding Engines to manage high traffic from CPE to internet. By default, this feature is disabled. Prior to Junos OS Release 19.2R1, you can assign an anycast address only to a single Packet Forwarding Engine and the maximum v4ov6 tunnel scale per Packet Forwarding Engine in MX Series is 150k. This restricts a single anycast address to be used for 150k tunnels.

To configure the same source address over multiple tunnel-attributes, use **set v4ov6 ipv6-anycast-source-duplication** statement at the **[edit routing-options dynamic-tunnels]** hierarchy level.

If v4ov6 packets are fragmented, the fragmented packets get steered to one of the anchor Packet Forwarding Engines for IPv6 reassembly processing. To steer the traffic to the correct anchor, Packet Forwarding Engine needs information about the range of IPv4 prefixes that goes over a particular tunnel. To get the range of IPv4 prefixes that goes over a particular tunnel, use set **get-route-range** statement at the **[edit policy-options policy-statement <policy-name> term <term-name> from route-filter <route-filter-value> <range>]** hierarchy level.

[See [v4ov6](#) and [get-route-range](#).]

- **Support for export of BGP Local RIB through BGP Monitoring Protocol (BMP) (MX Series)**—Starting in Junos OS Release 19.2R1, BMP is enhanced to support monitoring of local RIB (**loc-rib**) policy. The **loc-rib** policy is added to RIB types under the **bmp route-monitoring** statement.

[See: [Understanding the BGP Monitoring Protocol](#).]

- **Support for BGP routes with N-Multipath primary and 1-Protection backup gateway (MX Series)**—Starting in Junos OS 19.2R1, the following enhancements are made to the Junos OS:
 - Support N+1 formation for BGP labelled unicast protection (LU).
 - Support N+1 formation for BGP PIC (IPv4, IPv6, LU).
 - Support for hetero-nexthops (ListNH) in such N+1 formations.
 - Support for KRT to defer fib-update if BGP-multipath is in progress.
 - Removed restriction to use **delay-route-advertisement** statement for IPv4 labeled-unicast.
 - Four new options **import**, **install-address <address>**, **no-install**, and **rib (inet.0 | inet6.0)** are added under the **egress-te** statement.
 - A new configuration statement **allow-protection** is introduced to allow protection for multipath legs. To allow protection for multipath legs, use **set allow-protection** statement at the **[edit protocols bgp multipath]** hierarchy level.
 - A new option **always-wait-for-krt-drain** is introduced under **delay-route-advertisement** statement to make more-specific BGP-routes re-advertisement to wait for KRT-queue to drain. To configure this, use **set always-wait-for-krt-drain** at the **[edit protocols bgp family inet unicast delay-route-advertisements]** hierarchy level.

[See [allow-protection \(Multipath\)](#), [delay-route-advertisements](#) and [egress-te](#).]

Security

- **Juniper Malware Removal Tool**—Starting in Junos OS Release 19.2R1, the Juniper Malware Removal Tool (JMRT) can be used to scan and remove malware running on Junos OS devices. To run JMRT, use the operational commands under the **request system malware-scan** hierarchy. There are 2 types of scans you can perform with JMRT:

Quick—Scan each running program file.

Veriexec check—Check if verified execution is enabled.

[See [request system malware-scan](#).]

Services Applications

- **Support for IPv6 BGP next-hop address in IPv6 and MPLS-IPv6 inline flow record templates(MX Series)**—Starting in Junos OS Release 19.2R1, a new element, IPv6 BGP NextHop Address, is available in the the IPv6 inline flow record template and the MPLS-IPv6 inline flow record template to add support for IPv6 BGP NextHop information element. The new element is supported on both version 9 and version 10 (IPFIX) export formats. The element ID is 63 and the element size is 16 bytes.

[See [Understanding Inline Active Flow Monitoring](#).]

- **IPv4 and IPv6 version 9 templates for inline active flow monitoring (MPC10E-15C-MRATE on MX Series)**—Starting in Junos OS Release 19.2R1, while configuring inline active flow monitoring, you can apply version 9 flow templates to define a flow record template suitable for IPv4 or IPv6 traffic.

[See [Configuring Flow Aggregation on MX, M, vMX and T Series Routers and NFX250 to Use Version 9 Flow Templates](#).]

- **Support for Two-Way Active Measurement Protocol (TWAMP) on MPC10E-15C-MRATE line card**—Starting in Junos OS Release 19.2R1, TWAMP is supported on MPC10E line card on the MX240, MX480, and MX960 routers. TWAMP defines a standard for measuring IPv4 performance between two devices in a network. You can use the TWAMP-Control protocol to set up performance measurement sessions between a TWAMP client and a TWAMP server, and use the TWAMP-Test protocol to send and receive performance measurement probes.

Configuring the TWAMP client instance to use *si-x/y/z* as the destination interface (which enables inline services) is not supported if the router has an MPC10E-15C-MRATE installed in the chassis. You can configure only the **none** authentication mode on the line card.

[See [Understanding Two-Way Active Measurement Protocol on Routers](#).]

- **DS-Lite support on MX Virtual Chassis and MX BNG**—Starting in Junos OS Release 19.2R1, the MX Series Virtual Chassis and MX Series broadband network gateway (BNG) support dual-stack lite (DS-Lite). DS-Lite uses IPv4-over-IPv6 tunnels to traverse an IPv6 access network to reach a carrier-grade IPv4-IPv4 NAT. DS-Lite enables the phased introduction of IPv6 on the Internet by providing backward compatibility with IPv4.

DS-Lite on the MX Series Virtual Chassis and MX Series BNG does not support the following:

- Application Layer Gateways (ALGs)
- Limits per subnet
- Clearing NAT mappings and flows for a specific subscriber, for a basic bridging broadband device (B4), or for a specific service set
- Port Control Protocol

[See [Tunneling Services for IPv4-to-IPv6 Transition Overview](#).]

- **Hardware timestamping of RPM probe messages**—Starting in Junos OS Releases 19.2R1, you can enable timestamps on RPM probes messages in the Packet Forwarding Engine host processor for the following line cards:
 - MPC10E-15C-MRATE line card on MX240, MX480, and MX960 routers
 - MPC11E line card on MX2008, MX2010, and MX2020 routers

You can use the following configuration statements at the `[edit services rpm probe owner test test-name]` hierarchy level:

- **hardware-timestamp**—Enables timestamping of RPM probe messages in the Packet Forwarding Engine host Processor.
- **one-way-hardware-timestamp**—Enables timestamping of RPM probe messages for one-way delay and jitter measurements.

These configuration statements are supported only with icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types.

See [\[hardware-timestamp\]](#)

[\[one-way-hardware-timestamp\]](#)

[Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX and MX Series Routers](#)

- **Increased number of AMS members supported on single chassis (MX2020)**—Starting in Junos OS Release 19.2R1, you can configure up to 60 MS-PICs as part of aggregated multiservices (AMS) bundles on a single chassis. The configuration supports backup and load-balancing mode (N:1) and all active mode (N:0) with both next-hop style services and interface style services of configurations.

See [\[Understanding Aggregated Multiservices Interfaces\]](#).

- **IPFIX flow-cache support (MX150)** —Starting in Junos OS Release 19.2R1, the flow cache infrastructure support is extended to IPFIX to provide improved throughput with IPFIX service enabled. In earlier releases, without flow cache support for IPFIX, all data traffic would take the microcode path which is much slower than flow cache. With this feature, the unsampled traffic gets forwarded using flow cache which results in better throughput.

Software Defined Networking

- **PCE-initiated bypass LSPs (MX Series)**—Starting in Junos OS Release 19.2R1, the Path Computation Element Protocol (PCEP) functionality is extended to allow a stateful Path Computation Element (PCE) to initiate, provision, and manage bypass label-switched paths (LSPs) for a protected interface. Multiple bypass LSPs with bandwidth reservation can be initiated by the PCE to protect a resource.

With this feature, you can benefit from the LSP state synchronization of manual, dynamic, and PCE-initiated bypass LSPs from a PCE, and leverage on the PCE's global view of the network, resulting in better control over traffic at the time of a failure, and deterministic path computation of protection paths.

[See [Support of the Path Computation Element Protocol for RSVP-TE Overview](#).]

- **Support for unified ISSU on abstracted fabric interfaces (MX480, MX960, MX2010, MX2020, MX2008)**—Starting in Junos OS Release 19.2R1, abstracted fabric (af) interfaces, configured for Junos Node Slicing, support unified in-service software upgrade (ISSU). Unified ISSU enables an upgrade between two Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

NOTE: Since the af interface traffic is load balanced across all available Packet Forwarding Engines, the traffic loss on an AF interface during ISSU might be higher, compared to the traffic loss on a regular interface.

An af interface is a pseudo interface that represents a first class Ethernet interface behavior. An AF interface facilitates routing control and management traffic between guest network functions (GNFs) through the switch fabric.

[See [Abstracted Fabric \(AF\) Interface](#).]

- **Centralized assignment of unique MAC addresses to GNFs (MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 19.2R1, Junos node slicing supports the assignment of a globally unique MAC address range (supplied by Juniper Networks) for GNFs. To receive the globally unique MAC address range for the GNFs, contact your Juniper Networks representative and provide your GNF license SSRN (Software Support Reference Number), which will have been shipped to you electronically upon your purchase of the GNF license. For each GNF license, you will then be provided an 'augmented SSRN', which includes the globally unique MAC address range assigned by Juniper Networks for that GNF license. You must then configure this augmented SSRN at the JDM CLI as follows:

set system vnf-license-supplement vnf-id *gnf-id* license-supplement-string *augmented-ssrn-string*.

[See [Assigning MAC Addresses to GNF](#)]

- **Support for IPSec, stateful firewall, and CGNAT services on MS-MPCs over abstracted fabric interfaces (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 19.2R1, guest network functions (GNF) support Layer 3 services such as Carrier-Grade Network Address Translation (CGNAT), stateful firewall, and IP Security (IPsec) on Multiservices MPCs (MS-MPCs) over abstracted fabric (af) interfaces.

[See [Abstracted Fabric Interface](#)]

- **MX2008 routers support in-chassis Junos node slicing (MX Series)**—Starting in Junos OS Release 19.2R1, MX2008 routers support the in-chassis model of Junos node slicing deployment. In the in-chassis model, the base system (BSYS), Juniper Device Manager (JDM), and all guest network functions (GNFs) run within the Routing Engine of the MX Series router. To support in-chassis Junos node slicing, the MX2008 must have the Routing Engine REMX2008-X8-128G installed.

[See [Configuring MX Series Router to Operate in In-Chassis Mode](#)]

Software Installation and Upgrade

- **The curl binary is packaged and made available on all Junos OS variants (MX Series)**—The curl binary is a command-line utility, used from the shell, that you can use to perform operations over several transport protocols, including the following: dict, file, ftp, gopher, http, imap, pop3, rtsp, smtp, telnet, tftp. The features enabled on Junos OS are curl version 7.59, libcurl version 7.59.

Subscriber Management and Services

- **Support for M:N subscriber redundancy on BNGs (MX Series)**—Starting in Junos OS Release 19.2R1, you can configure broadband network gateways (BNGs) to provide interface-level redundancy for DHCP subscribers that are on the same static VLAN and use the same access interface. Failover from master to backup BNG is transparent to the clients because the subscriber sessions remain up. You must configure DHCP active leasequery with topology discovery on peer DHCP relay agents on the master and backup BNGs to support the redundancy.

[See [M:N Subscriber Redundancy](#).]

- **Support for Interface-Level Redundancy with DHCP Topology Discovery (MX Series)**—Starting in Junos OS Release 19.2R1, you can configure DHCP active leasequery with topology discovery to provide interface-level subscriber redundancy between peer relay agents. Topology discovery enables master and backup peer relay agents to determine the access interfaces on peers that correspond to their own local access interfaces for servicing subscriber redundancy groups. During synchronization, DHCP translates the subscriber binding information to use the local interface on the backup instead of the interface on the master. You must use topology discovery when you configure M:N subscriber redundancy.

[See [DHCP Active Leasequery](#).]

- **Support for fixed wireless access subscribers on BNGs (MX Series)**—Starting in Junos OS Release 19.2R1, you can configure the broadband network gateway (BNG) to support subscribers that use a fixed wireless network. Providers use a wireless network for subscriber access over the air instead of than running fiber to the home. The wireless infrastructure saves costs and reduces complexity compared to the fiber network. The BNG acts as the Third-Generation Partnership Project (3GPP) System Architecture Evolution Gateway (SAEGW). The SAEGW incorporates the functions of both the Serving Gateway (SGW) and the Packet Data Network Gateway (PGW). The SGW function routes and forwards user data packets. The PGW function provides connectivity to external packet data networks

[See [Fixed Wireless Access Networks](#).]

System Management

- **Support for transferring accounting statistics files and router configuration archives using HTTP URL (MX Series)**—Starting in Junos OS Release 19.2R1, you can transfer accounting statistics files and router configuration archives to remote servers by using an HTTP URL. In addition to SCP and FTP, the following HTTP URL will be supported under the **archive-sites** statement:

```
http://username@host:url-path password password
```

- To transfer accounting statistics files, configure **archive-sites** under **[edit accounting-options file <filename>]** hierarchy.
- To transfer router configuration archival, configure **archive-sites** under **edit system archival configuration** hierarchy.
- To view the statistics of transfer attempted, succeeded, and failed, use the **show accounting server statistics archival-transfer** command.
- To clear the statistics of transfer attempted, succeeded, and failed, use the **clear accounting server statistics archival-transfer** command.

[See [archive-sites](#), [Backing Up Configurations to an Archive Site](#), [show accounting server statistics archival-transfer](#), and [clear accounting server statistics archival-transfer](#)].

Timing and Synchronization

- **Support for Synchronous Ethernet with ESMC on MPC10E-15C-MRATE (MX240, MX480, MX960)**—Starting in Junos OS Release 19.2R1, MPC10E-15C-MRATE supports Synchronous Ethernet with ESMC. Synchronous Ethernet is a physical layer technology that is used to transfer clock signals over Ethernet interfaces. It supports hop-by-hop frequency transfer, where all interfaces on the trail must support Synchronous Ethernet.

ESMC is a logical communication channel. It transmits Synchronization Status Message (SSM) information, which is the quality level of the transmitting synchronous Ethernet equipment clock (EEC), by using ESMC protocol data units (PDUs).

[See [Synchronous Ethernet Overview](#)].

SEE ALSO

What's Changed 96
Known Limitations 100
Open Issues 102
Resolved Issues 111
Documentation Updates 129
Migration, Upgrade, and Downgrade Instructions 130

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 96](#)
- [MPLS | 97](#)
- [Network Management and Monitoring | 97](#)
- [Routing Policy and Firewall Filters | 98](#)
- [Services Applications | 98](#)
- [Software Defined Networking | 98](#)
- [Subscriber Management and Services | 98](#)
- [VLAN Infrastructure | 99](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for MX Series routers.

Interfaces and Chassis

- **Deprecation of the [edit fabric protocols bgp] hierarchy level (MX Series)**—Starting in Junos OS Release 19.2R1 and later, the [edit fabric protocols bgp] hierarchy level is deprecated.
- **Support to get Optics Loopback Status for QSFP-100GE-DWDM2 transceivers (MX Series)**—In Junos OS Release 19.2R1, and later, on MX Series routers, you can get the optics loopback status of QSFP-100GE-DWDM2 transceivers along with the regular ethernet loopback status by issuing the **show interfaces *interface-name*** or **show interfaces *interface-name* brief** command. New Output field **Optics Loopback** is added under **Link-level type** when **show interfaces *interface-name*** CLI command is executed.
- **Monitoring information available only in Trace log (MX Series)**—In Junos OS Release 19.2R1 and later, the Ethernet link fault management daemon (lfmd) in the peer router stops monitoring the locally occurred errors until ISSU completes. You can view the monitoring-related details only through the trace log file.
- **Health check for power supplies (MX10008 and MX10016)**—Starting in Junos OS Release 19.2R1, on the MX10008 and MX10016 routers, the **show chassis environment pem** command displays the health check information about the DC or AC Power supplies. For any power supply that does not support health check, the status is shown as **Unsupported**. The system starts health check of a power supply only if the power consumption exceeds 7 KW.

[See [show chassis environment pem](#)]

MPLS

- **New debug statistics counter (MX Series)**—The `show system statistics mpls` command has a new output field, called **Packets dropped, over p2mp composite nexthop**, to record the packet drops over composite point-to-multipoint next hops.

Network Management and Monitoring

- **The show system schema command and <get-yang-schema> RPC require specifying an output directory (MX Series)**—Starting in Junos OS Release 19.2R1, when you issue the `show system schema` operational mode command in the CLI or execute the `<get-yang-schema>` RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the `<output-directory>` element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type empty (MX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are only supported when executing the RPC in a NETCONF or Junos XML protocol session, and the value passed to the action script is the string '**none**'.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

- **Change in power supply alarms (MX10003)**—Starting in Junos OS Release 19.2R1, the MX10003 routers do not raise an alarm if a Power Entry Module (PEM) slot is empty. However, when the number of operational PEMs available is less than 2, the router raises a major alarm. This alarm is cleared when the required number of PEMs are made available.

[See [show chassis alarms](#)]

Routing Policy and Firewall Filters

- **Fixed an issue with certain combination of match conditions**—In Junos OS Release 19.2R1, fixed a temporary issue wherein configuring a firewall filter with a match condition for **port** along with **source-port** and/or **destination-port** in the same filter term would cause a commit error. Any valid combination of the filter terms is now supported.

Services Applications

- **Support for host generated traffic on a GRE over GRE tunnel (MX Series)**—In Junos OS Release 19.2R1, you can send host generated traffic on a GRE over GRE tunnel. However, when path maximum transmission unit (PMTU) is updated for the outer GRE tunnel, MTU for inner GRE tunnel is not corrected.
- **New syslog message displayed during NAT port allocation error (MX Series Routers with MS MPC)**—With address pooling paired (APP) enabled, an internal host is mapped to a particular NAT pool address. In case, all the ports under a NAT pool address are exhausted, further port allocation requests from the internal host results in a port allocation failure. The following new syslog message is displayed during such conditions:

JSERVICES_NAT_OUTOF_PORTS_APP

This syslog message is generated only once per NAT pool address.

Software Defined Networking

- **Deprecated CLI commands and options for JDM (MX480, MX960, MX2010, MX2020, and MX2008)**—Starting in Junos OS Release 19.2R1, in Junos Node Slicing, Juniper Device Manager (JDM) does not support the following CLI commands or options:
 - **show system visibility**
 - **show system inventory**
 - the **jinventoryd** option in the **restart** command

Subscriber Management and Services

- **Changing attributes of physical interface with active subscribers (MX Series)**—Starting in Junos OS Release 19.2R1, the commit check fails when you change any attribute of the physical interface, such as the MTU, when subscribers are active. This affects only aggregated Ethernet physical interfaces with targeted distribution configured. In earlier releases, the commit check does not fail and the attribute change brings down the physical interface and all subscribers using that interface.

[See [CoS for Aggregated Ethernet Subscriber Interfaces Overview](#).]

- **Out-of-address SNMP trap requires thresholds to be configured (MX Series)**—Starting in Junos OS Release 19.2R1, the behavior has changed for generating an out-of-address SNMP trap for an address pool. You must now configure both the high-utilization and abated-utilization thresholds. When the number of assigned addresses surpasses the high-utilization threshold, a high-utilization trap is generated. If all the addresses are assigned from the pool, an out-of-address trap is generated and an out-of-address syslog message is sent.

In earlier releases, an out-of-address trap is generated when the address pool is exhausted, regardless of whether the thresholds are configured.

[See [Configuring Address-Assignment Pool Usage Threshold Traps](#).]

VLAN Infrastructure

- **Specifying a descending VLAN ID range (MX Series routers, and vMX virtual routers)**—In Junos OS releases prior to Junos OS Release 19.2R1, the system accepts a descending range—for example, 102-100, with the **vlan-id-range** configuration statement in the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy.

Starting with Junos OS Release 19.2R1, the system considers a descending range specified with **vlan-id-range** to be invalid and raises an error if you try to commit this configuration.

SEE ALSO

[What's New | 76](#)

[Known Limitations | 100](#)

[Open Issues | 102](#)

[Resolved Issues | 111](#)

[Documentation Updates | 129](#)

[Migration, Upgrade, and Downgrade Instructions | 130](#)

[Product Compatibility | 137](#)

Known Behavior

IN THIS SECTION

- General Routing | 100
- Interfaces and Chassis | 101
- Routing Protocols | 102

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- The Routing Engine boots from the secondary disk when you: a) press the reset button, on the RCB front panel, while the Routing Engine is booting up but before Junos OS is up. b) Upgrade software, by booting from the network using the **request vmhost reboot network** command, and the system fails to boot from the network. c) Upgrade BIOS and the upgrade fails. d) Reboot and the system hangs before Junos OS is up. [PR1344342](#)
- During a unified ISSU that warrants host upgrade, if the router is configured with 8 million IPv4/IPv6 routes or more, the unified ISSU might fail resulting in FPC restart. [PR1348825](#)
- The MIC-MACSEC-20G supports 10-Gigabit speed through the **set chassis fpc x pic y pic-mode 10G** configuration applied to both the PICs in that MIC. Any other PIC mode configuration should be removed and then the 10-Gigabit PIC mode configuration is to be applied. [PR1374680](#)
- On MX2008 platform with MPC9E, in line rate traffic with a redundant SFB2 scenario, if offline one redundant SFB2, there might be tail or sometimes WRED drops in MPC9E, resulting in partial traffic loss. Under normal circumstances, the SFBs should be auto fail-over if one of them fails, and there should be only a little packet dropped momentarily. [PR1395591](#)
- The dfe tuning failing at times is a known issue on MX10003, the only recovery option in this situation is to restart the FPC. [PR1413233](#)
- In the following scenario Device 1 Remote Device **MX10003-mx1ru-h** <-----> **MX10003-mx3ru-i et-0/0/2 et-1/0/1**. If PRBS is started on simultaneously as TX and RX on both the devices, there will be errors seen at remote device because when PRBS is started as TX on remote device, it attempts to dfe tune the line again but PRBS is already running as RX which causes the error. So first start As Tx on

Device 1 and as Rx on Remote device, then stop the test on both the ends and start as TX on remote device and as Rx on Device 1. [PR1416124](#)

- Since creating the loopback at the MacSec port (remote end) in this specific situation, the link itself is down at the EA port hence PRBS test fails with incrementing error counts. [PR1421432](#)
- FLT will not support source-port and port combination match due to the limitation. [PR1432201](#)
- Dynamic spring-te tunnel creation to LDP (non SR) speaking nodes are not supported even in the presence of mapping server configurations. Spring-te internally converts the tunnel-hop IP addresses (prefix/adjacency) into corresponding labels through auto-translate feature. This feature internally makes use of Traffic Engineering Database (TED); where at present the mapping server entries are not present. [PR1432791](#)
- On MPC2 Junos telemetry interfaces services statistics might not be available after the unified ISSU. [PR1433589](#)
- 128k source-ip addresses as match condition should be configured under couple terms. After commit the configuration, it will take 10 minutes to effect. [PR1433974](#)
- On MX10003 platform with no MSATA device, xSTP topology change is seen during FRU upgrade state in unified ISSU. [PR1435397](#)
- When the Junos telemetry interface collector runs for a longer duration, the iLatency will be negative. [PR1436126](#)
- Whenever the primary path goes down for the SRTE tunnel, dynamic tunnel module (DTM) starts an expiry timer of 15 minutes. If the primary path comes up within this timer period, the tunnel will be up again. After the timer expires and the primary path is still not up, DTM asks SRTE to remove the tunnel. Also, if there are multiple paths to reach the tunnel endpoint, bgp routes will resolve over the other route, for example a L-ISIS path. Later even if the primary path comes up, bgp routes will remain resolved over the other secondary route and does not change. No re-resolution is happening because the SRTE tunnel is resolving with more than one indirection (SRTE over MPLS over IS-IS in this case). Because of the whole design of how resolution happens and multiple dependencies, there is no simple fix for this. The same issue is applicable to RSVP tunnels also. The issue is applicable to uncolored tunnels only. [PR1439557](#)
- Interworking between MPC10E and SCBE3 is not supported. [PR1440073](#)

Interfaces and Chassis

- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfmd process to crash after upgrade. This is because of the presence of an old version of `/var/db/cfm.db`. [PR1281073](#)
- When disabling physical interface with JNP-100G-AOC-xM AOC cables, port LED could turn red or go off depending on vendor. JNP-100G-AOC-xM cables sourced by Finisar will cause port LED to turn red when physical interface is disabled. Cables sourced by Innolight will cause the port LED to turn off in

contrary. Transceiver vendor information can be obtained from the **show chassis pic fpc-slot <fpc slot> pic-slot<pic slot>** CLI command. Transceiver vendor field contains 'JUNIPER-FINISAR' for Finisar and 'JUNIPER-INNO' for Innolight. [PR1415958](#)

- Firmware upgrade for nPhi Madison optics is not supported on MX10008/16 Platform. [PR1424408](#)

Routing Protocols

- When 32,000 SRTE policies are configured at once, during configuration time there might be scheduler slips. [PR1339829](#)

SEE ALSO

[What's New | 76](#)

[What's Changed | 96](#)

[Open Issues | 102](#)

[Resolved Issues | 111](#)

[Documentation Updates | 129](#)

[Migration, Upgrade, and Downgrade Instructions | 130](#)

[Product Compatibility | 137](#)

Known Issues

IN THIS SECTION

- [EVPN | 103](#)
- [Forwarding and Sampling | 103](#)
- [General Routing | 104](#)
- [Interfaces and Chassis | 108](#)
- [Layer 2 Ethernet Services | 109](#)
- [MPLS | 109](#)
- [Platform and Infrastructure | 109](#)
- [Routing Protocols | 110](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- Replace multihome advertisement proxy bit from the L2_info community to the ARP/ND extended community. The default value is 0x4. [PR1408055](#)
- In an EVPN-VXLAN scenario with scaled bridge domains configured (for example, 4000 bridge domains), if the core-facing link on the VTEP (VXLAN tunnel endpoint) comes up (Down >> Up), the traffic received from the customer edge might be dropped by the VTEP for a period of time before it becomes normal. [PR1408840](#)
- In an EVPN A/A ESI multihoming scenario with dynamic list next hop used, the next hop is not cleaned up properly on the remote PE device when one of the multihomed CE-PE links goes down. The unavailable next hop leads to packets loss for user traffic. [PR1412051](#)
- In an EVPN single active scenario, the [EVPN/7] /32 host route always appears on non-DF PE if chained composite next hop (chained CNH) is enabled. The **protocols evpn remote-ip-host-routes** configuration has no effect if chained CNH is enabled. If chained CNH is disabled, the **remote-ip-host-routes** configuration has the intended effect. [PR1419466](#)

Forwarding and Sampling

- The **skip-service** configuration does not work with IPv6 NDP negotiation or ping. [PR1074853](#)
- The SRRD process acts as a server for all active Junos Traffic Vision (previously known as J-Flow) for flow monitoring clients. The active flow monitoring clients can be either Packet Forwarding Engines or PICs performing flow monitoring. The maximum number of active flow monitoring clients was previously 32 and the number has been increased to 64 in this release. [PR1261783](#)
- If an IPv4 prefix is added to a prefix-list referred by an IPv6 firewall filter then the log message **Prefix-List [Block-Host] in Filter [Protect_V6] not having any relevant prefixes , Match [from prefix-list Block-Host] might be optimized** is not seen. [PR1395923](#)
- In the case of a physical interface policer for ip-option traffic, the traffic rate is found to be more than 10 percent. . [PR1398728](#)

General Routing

- If a Layer 3 interface is receiving a GRE encapsulated packet and interface has the following two filters attached in ingres: 1) **family any** with action as **mirror** 2) **family inet** with action as **decapsulate gre**, then the expected behavior is that the mirrored copy must have the GRE headers as well. However, the configuration is not working as expected due to presence of the **family-inet** filter. If the user is interested in mirroring entire packets that reach the interface (that includes GRE header as well), then workaround is to deactivate or disable the **decapsulate gre** action of that filter. [PR1090854](#)
- Load balancing is uneven across aggregated Ethernet member links when the aggregated Ethernet bundle is part of an ECMP path. The aggregated Ethernet member links need to span Virtual Chassis members. [PR1255542](#)
- The following cosmetic error is observed as the output: **mspanmand[190]: msvcs_session_send: Plugin id 3 not present in the svc chain for session.**[PR1258970](#)
- The deletion of oneset/Leaf-list configuration through JSON might not get deleted when the “delete” attribute is passed in the JSON string. [PR1287342](#)
- MPLS over GRE dynamic tunnel localization does not work when chained composite next-hop is enabled. [PR1318984](#)
- With regard to FPC restarts or Virtual Chassis splits, the design of MX Series Virtual Chassis infrastructure relies on the integrity of the TCP connections, and the reactions to failure situation might not be handled in a graceful way. The TCP connection timeout occurs because of the jlock hog crosses the boundary value (5seconds), causing bad consequences in the MX Virtual Chassis. [PR1332765](#)
- The output of the **show class-of-service fabric statistics** command now includes traffic that was dropped because of internal errors in the drop counts. [PR1338647](#)
- The first packet pertaining to active Flow Packet Forwarding Engine sensor in UDP mode is missing after a line-card reboot on MX150 routers. [PR1344755](#)
- With GRES enabled in a subscriber environment, if subscribers are logging in or out very quickly, the service sessions in the session database (SDB) of the backup Routing Engine might be leaked. If the problem is not detected for long enough, the backup Routing Engine might not be able to come back into synchronization with the master Routing Engine and will not be ready for GRES. [PR1346300](#)
- On next generation Routing Engine, a failure of the hardware random number generator (HWRNG) will leave the system in a state where not enough entropy is available to operate. [PR1349373](#)
- If the packets are destined to specific MAC address (for example, if the last two octets are 0x1101, 0x1102, 0x1103, 0x1104, 0x1106, 0x1108, 0x1109, 0x110a and so on), they might be dropped on the remote-end device when going through the built-in 10-Gigabit Ethernet (xe-) ports on the MX104 device. [PR1356657](#)
- When the FPC is booting up (either during unified ISSU or router reboot or FPC restart), I2C timeout errors for SFP are noticed. These errors are seen because the I2C action is not completed as the device

was busy. After the FPC is up, all the I2C transactions to the device were normal, so no periodic failure is observed. There is no functional impact and these errors can be ignored. [PR1369382](#)

- Users can issue the **set vmhost...** command although **permissions system-control** is not configured on the system class. [PR1383706](#)
- After adding additional sites to existing group and routing instance configuration, configuration commit check might fail with the following error: **abcdef# commit check re0: [edit routing-instances ELAN-XYZ protocols vpls site ABC-xe-0/3/2-site17 interface] 'xe-0/3/2.1522' Interface must be part of this routing instance error: configuration check-out failed: (statements constraint check failed)** [PR1391668](#)
- The **ether-pseudowire zero-control-word** configuration option under the **forwarding-options enhanced-hash-key family mpls** statement does not take effect in a Junos node slicing setup. Although configured using the **set forwarding-options enhanced-hash-key family mpls ether-pseudowire zero-control-word** statement, the parameter is not passed to the MPC9E line card. This can impact load balancing over abstracted fabric (AF) interfaces when you use the pseudowire headend termination (PWHT) in a guest network function (GNF). [PR1400881](#)
- In a BGP Prefix Independent Convergence (PIC) case, If a route R1 resolves on top of the multipath route R2, where R2 has primary and backup indirect next hops, it will be better if the backup leg is not used for the resolution of R1. There is no impact on any existing CLI commands. The backup path is never used when the primary path is available. [PR1401322](#)
- The rpd process might crash and generate a core file while rebooting when **condition-manger policy** is configured for routing table xxx and the same table is repeatedly deleted and readded. [PR1401396](#)
- In a JET/telemetry scenario, the telemetry log file is not rotated and keeps growing until the Routing Engine is out of disk space, which might cause unexpected impact of the Routing Engine, and eventually lead to a Routing Engine crash. [PR1401817](#)
- The rpd process might crash after a nonforwarding route (that is, a route to an indirect next-hop association is a nonforwarding indirect next- hop) that is received from multiple protocols is resolved again by using the nonforwarding path. [PR1407408](#)
- On vMX-based platforms including MX150, when you run the **clear pim join instance instance-name all** command, it might result in stopping of the riot process on the system. [PR1409527](#)
- Configuration database might remain locked after the SSH session is halted. [PR1410322](#)
- A small number of tunneled subscribers might be terminated during unified ISSU because of momentary loss of IP connectivity between the LAC and LNS devices. [PR1414928](#)
- FPC core files are seen when hierarchical CoS is added to and deleted from pseudo wire devices multiple times. This issue can be circumvented by removing the psuedowire device without changing hierarchical the CoS configuration. [PR1414969](#)
- cRPD does not restrict the number of simultaneous JET API sessions. [PR1415802](#)
- The Packet Forwarding Engine on the MX Series does not account for the labels pushed onto the packet on the egress Packet Forwarding Engine, while Packet Forwarding Engine on the PTX Series device does. This results in a slight difference in the byte count for the same traffic stream across these two platforms.

The packet count will still be the same across the platforms. Currently, this issue is noticed for uncolored SRTE policies. [PR1416738](#)

- The rpd process might generate a core file when a user initiates a restart or when deactivating a logical system. The crash is seen only when the rpd process terminates or shutdown. The impact on network is minimal. [PR1418192](#)
- Changing CAK and CKN multiple times within shorter interval (approximately 5 minutes) sometimes **show security macsec connection** inbound and outbound channel display more than one AN active. But in Packet Forwarding Engine hardware side correct AN and SAK is programmed and MKA protocol from both end transmit correct and latest AN on each hello packets. [PR1418448](#)
- The **show services hybrid-access sessions**, **show services hybrid-access statistics**, and **show services hybrid-access tunnels** commands display values of zero for hybrid access gateway traffic statistics even when traffic is active in the gateway sessions and the tunnels. [PR1419529](#)
- Certain JNP10008-SF and JNP10016-SF switch interface boards (SIBs) manufactured between July 2018 and March 2019 might have incorrect core voltage setting. The issue can be corrected by reprogramming the core voltage and updating the setting in nvram memory. [PR1420864](#)
- When you create the loopback at the MACsec port (remote end) in this specific situation, the link itself is down at the EA port hence the pseudo random binary sequence (PRBS) test fails with incrementing error counts. [PR1421432](#)
- vMX RIOT process panics. As a result, RIOT core file is generated that impacts data forwarding. During this condition, following logs are seen in the log messages: **May 23 18:00:07 fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): May 27 05:41:21 fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc()**. [PR1423575](#)
- Junos OS Releases 19.1 and later support RFC 8231/8281 compliance by default. However, if the controller is not compliant with RFC 8231/8281, backward compatibility can be configured to fall back to pre-RFC 8231/8281 behavior. [PR1423894](#)
- More number of MACs/MAC-IPs can get learnt if **mac-limit** or **mac-ip limit** is configured in a particular sequence. An example is shown below: 1. Learn 50 remote entries 2. Configure **mac-limit** of 20 (remote entries remain intact, this works as expected) 3. Learn 50 local entries At this point, no local entries must be learnt, as MAC limit is 20. However, all 50 local MACs get learnt causing MAC count to be 100, which is incorrect. The same issue will be seen for **mac-ip limit** as well. [PR1428572](#)
- Due to a race condition between the creation of logical interfaces and GARP packet sent out when a logical interface is configured, there is an issue of one output packet logical interface statistics increment. [PR1430431](#)
- With old midplane and with mpc10e-15c, if the configuration **set chassis fpc <num> pfe 2 power off** is used to make it two Packet Forwarding Engine system, then on restarting the line card, destination errors are observed on all fabric planes for both PFE0 and PFE1 and eventually FPC might go offline because of the fabric hardening actions. [PR1432019](#)

- Deleting the configuration **chassis license bandwidth** (in case of Agile licensing model) will not cause device to default to maximum bandwidth available or entitled. [PR1433157](#)
- Few entries are specific to **show dynamic-tunnels database** output are not getting populated with testing the functionality after online or offlining of pic. [PR1433247](#)
- When **GNMI set RPC** is executed from GNMI clients with 'replace' field, MGD-API process crashes and generates a core file. All other fields with **set RPC** works fine. Issue is seen only when 'replace' field exists in request. As a workaround, 'replace' field is used **replace config element sub-hierarchy** with new element sub-hierarchy. For example, [To replace 'area 0.0.0' sub-hierarchy with 'area 1.1.1.1'] that is, **set protocols ospf area 0.0.0.0 interface fxp0.0**. To set protocols ospf area 1.1.1.1 interface lo0.0, you can use 'replace' field to achieve this. But, the same operation can be achieved having both 'delete' and 'update' fields in single RPC request. That is, **single set RPC** with below fields 'delete' field has 'delete protocols ospf area 0.0.0.0' 'update' field has **set protocols ospf area 1.1.1.1 interface lo0.0**. [PR1433378](#)
- From Junos OS Release 18.2 and later, **DTCP enable** command to add drop policy for a mirrored subscriber does not work. In Junos OS Release 18.2, mirroring for subscriber will continue to happen, but drop policy does not get applied. From Junos OS Release 18.3 and later, subscriber mirroring might also get affected after **DTCP enable** command. [PR1435736](#)
- Subscriber interim statistics might reset to 0 in MX Series Virtual Chassis setup after GRES. [PR1436419](#)
- With scaled inline single hop BFD sessions, and events such as restart of FPC/ppmd/rpd, some of the BFD sessions might flap. [PR1436543](#)
- The **my-mac-check-failed exception counter** display is missing from the CLI output. But the functionality is working as expected. [PR1438761](#)
- The interface-specific filters do not take effect on MPC10E line cards, across the Packet Forwarding Engines. It is advisable not to use ISFs in this release. [PR1439327](#)
- Before switching mastership of Routing Engine, need to wait minimum of 4 minutes after enabling the GRES configuration for both the Routing Engines to come up in dual Routing Engine mode. Check GRES readiness by executing both **request chassis routing-engine master switch check** command from the master Routing Engine and **show system switchover** command from the backup Routing Engine. [PR1439884](#)
- There is a change in the way egress topology is been setup for the control packets in MPC10 than legacy MX Series routers. In legacy MX Series routers, the control packets (ARP) are not subject to family any firewall next-hops, whereas in MPC10 it will be. Thus, if the firewall do not have the ACCEPT default term, it is expected to drop the ARP packet. [PR1440792](#)
- After manually disabling and enabling aggregated Ethernet interface, it takes about 15 seconds for the LACP to converge and aggregated Ethernet interface to come up. [PR1441255](#)
- Firmware upgrade for PSU (JNP10K-AC2) and JNP10K-DC2) on MX10000 and PTX10000 systems with Routing Engine redundancy configuration enabled might fail because lcmd being disabled by the firmware upgrade command. [PR1452324](#)

Interfaces and Chassis

- Out-of-sequence packets are seen with the LSQ interface. [PR1258258](#)
- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfmd process to crash after upgrade. This is because of the presence of the old version of `/var/db/cfm.db`. [PR1281073](#)
- Some routers index the SFP transceivers starting at 1, while interface numbering starts from 0; thus, reading the Packet Forwarding Engine-level output can be confusing. [PR1412040](#)
- When an unnumbered interface is binding to an interface that has more than one IP address and one of the IP addresses is deleted, the family **inet** of the unnumbered interface might be getting deleted. The issue results in traffic loss for all the services that rely on the family **inet** of the unnumbered interface. Configuring **preferred-source-address** on the unnumbered interface will prevent deletion of the IP addresses, thus, avoiding the deletion of the family **inet** of the unnumbered interface. [PR1412534](#)
- If an aggregated Ethernet interface has VRRP configuration, in following use cases, member logical interfaces will not be created after member physical interface comes up and aggregated Ethernet will be in down state.
 - fpc restart (request chassis fpc restart slot < >)
 - chassis-control restart (restart chassis-control)
 - reboot both RE (request system reboot both-routing-engines)

So, before performing the above operations, it is advisable to remove VRRP configuration from the aggregated Ethernet interface. [PR1429045](#)

- Discrepancy of bytes and packets count in Routing Engine CLI for traffic and transit statistics, output of below two commands is changed in Junos OS Release 19.2R1 on AFT cards. On legacy cards output remains the same. **show interfaces xe-0/0/0:0.0 statistics** displays the input and output rate instead of input and output packets. The following commands shows the rate for traffic statistics (total traffic) instead of transit statistics. **show interfaces xe-0/0/0:0.0 statistics detail Show interface xe-0/0/0:0.0 extensive**. [PR1435416](#)
- From Junos OS Release 18.2 and later, **DTCP enable** command that is used to add drop-policy for a mirrored subscriber does not work. In Junos OS Release 18.2, mirroring for subscriber will continue to happen, but drop-policy does not get applied. From Junos OS Release 18.3 and later, the subscriber mirroring will also get affected after **DTCP enable** command. [PR1435736](#)

Layer 2 Ethernet Services

- **fpc3 user.err aftd-trio: [bt] #1 JnhHandle:** error messages been logged. Now issue is not seen with latest build [PR1424106](#)

MPLS

- With nonstop active routing (NSR), when the routing protocol process (rpd) restarts on the master Routing Engine, the rpd on the backup Routing Engine might restart. [PR1282369](#)

Platform and Infrastructure

- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log the error as **nh_ucast_change:291Referenced l2ifl not found**. This condition should be transient, with the system reconverging on the expected state. [PR1054798](#)
- An accuracy issue occurs with three-color single-rate and two-rate policers in which the policer rate and burst-size combination of the policer accuracy vary. This issue is present on all MX Series devices with MPCs and MICs. [PR1307882](#)
- There are multiple failures when events like node reboots, ICL flaps and ICCP flap occur even with **enhanced convergence** configured. There will be no guarantee that sub-second convergence will be achieved. [PR1371493](#)
- If scaling IFLSet members and aggregated Ethernet members are configured on the same FPC, the FPC might crash when it restarts. [PR1380527](#)
- During unified ISSU, the MX Series router displays an unnecessary **Can't assign requested address** syslog message for addresses associated with the NTP server. You can ignore this log message as it has no consequence. [PR1422545](#)
- After GRES a few ARP entries are not seen. When the interface flaps, the ARP entries are seen again. [PR1429983](#)
- On MX Series routers enabled with GRES and NonStop Routing (NSR) on both end of BGP peer, in scaled BGP session setup, BGP peers might flap after the execution of Routing Engine mastership switchover on both the boxes simultaneously. [PR1437257](#)
- With Junos OS Release 19.2R1, the EVPN-VXLAN packets egressing IRB might get dropped with traps when there are multiple Packet Forwarding Engines involved. [PR1439068](#)

Routing Protocols

- LDP and OSPF are in the in sync state and the reason observed for this is that the IGP interface is down with LDP synchronization enabled for OSPF. `user@host> show ospf interface ae100.0 extensive` Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. According to the current analysis, **IGP interface down** is observed as the reason because although LDP notified OSPF that LDP synchronization was achieved, OSPF was not able to take note of the LDP synchronization notification, because the OSPF neighbor was not up yet. [PR1256434](#)
- With Bidirectional Forwarding Detection (BFD) configured on an aggregated Ethernet interface, if you disable/enable the aggregated Ethernet interface, then that interface and the BFD session might not come up. [PR1354409](#)
- Its possible for a GNF with rosen6 multicast to display stuck KRT queue entries after recovery from a dual Routing Engine reboot at the BSYS. [PR1367849](#)
- When the loopback interface is configured in a logical system and Routing Engine-based micro-BFD is configured to use the loopback address as source address, BFD packets go out with the source address belonging to outgoing interface rather than the loopback address. Due to this issue, the micro-BFD session might not be able to come up. [PR1370463](#)
- On all Junos OS platform enabled with GRES and Non Stop Routing (NSR), if Routing Engine switchover is executed, the BGP peers in the new master Routing Engine might flap because of the hold-timer expiry after GRES. [PR1390113](#)
- Memory leak of around 300,000 routes occur when the remote-operations daemon is running and when around 2000 flow-spec routes were distributed. [PR1401914](#)
- Day-one design for BGP NSR. This issue is not specific to this release and can be seen on any of the older Junos OS releases. During NSR initial state replication in a scaled setup, there could be cases where while BGP state replication is still ongoing and BGP task replication might get marked as completed. This is because BGP replication is triggered and controlled through the backup Routing Engine. Use the **show bgp replication** command to confirm that replication is actually completed. This corner case scenario is valid only in a scaled setup and during initial state synchronization. [PR1404470](#)
- In an MVPN scenario, the rpd might crash while removing multicast routes that do not have an associated (S,G) state or activating the **accept-remote-source** the configuration statement on PIM upstream interface. [PR1426921](#)
- In BGP graceful restart scenario, including helper mode which is enabled by default, rdp process might generate a core file because of the improper handling of BGP graceful restart stale routes during the BGP neighbor deleting. The rpd process might crash and service or traffic impact might occur. [PR1427987](#)
- In both GR helper and GR restarter scenarios, BFD down packets are not immediately sent. It might cause an issue where BGP session down is notified before BFD DOWN. [PR1432440](#)

- When a direct change of route distinguisher is done on a routing instance, the instance should be deactivated before changing RD and then reactivated again. [PR1433913](#)
- MVPN configuration removal from an VRF instance might result in generating an rpd core file as it is considered as a catastrophic change for routing daemon. Generating a core file can be avoided by following procedure:
 - deactivate the routing instance
 - commit the configuration
 - delete the mvpn config from the instance
 - commit the configuration -activate the routing instance [PR1434347](#)

SEE ALSO

[What's New | 76](#)

[What's Changed | 96](#)

[Known Limitations | 100](#)

[Resolved Issues | 111](#)

[Documentation Updates | 129](#)

[Migration, Upgrade, and Downgrade Instructions | 130](#)

[Product Compatibility | 137](#)

Resolved Issues

IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 112](#)
- [Authentication and Access Control | 112](#)
- [Class of Service \(CoS\) | 113](#)
- [EVPN | 113](#)
- [Flow-based and Packet-based Processing | 114](#)
- [Forwarding and Sampling | 114](#)
- [General Routing | 114](#)
- [Infrastructure | 121](#)
- [Interfaces and Chassis | 121](#)

- Layer 2 Features | 123
- Layer 2 Ethernet Services | 123
- MPLS | 123
- Network Management and Monitoring | 124
- Platform and Infrastructure | 125
- Routing Policy and Firewall Filters | 125
- Routing Protocols | 126
- Services Applications | 127
- Software Installation and Upgrade | 128
- Subscriber Access Management | 128
- User Interface and Configuration | 128
- VPNs | 128

This section lists the issues fixed in the Junos OS 19.2R1 Release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Application Layer Gateways (ALGs)

- DNS requests with the EDNS option might be dropped by the DNS ALG. [PR1379433](#)

Authentication and Access Control

- The dot1xd might crash when dot1xd receives incorrect reply length from the authd. [PR1372421](#)
- Push-to-JIMS now supports push auth entry to all online jims servers. [PR1407371](#)

Class of Service (CoS)

- Traffic drop occurs when deleting MPLS family or disabling the interface that has non-default EXP rewrite-rules. [PR1408817](#)

EVPN

- The rpd process would crash if deactivating the Autonomous-System (AS) in an EVPN scenario. [PR1381940](#)
- The RA packets might be sent out without using the configured virtual gateway address. [PR1384574](#)
- [EVPN/VXLAN] VTEP tunnel does not get deleted when EVPN peer goes down. [PR1390965](#)
- On EVPN setups, incorrect destination MAC addresses starting with 45 might show up when using the **show arp hostname** command. [PR1392575](#)
- The rpd process might crash with EVPN type-3 route churn. [PR1394803](#)
- The rpd process generates core files upon Routing Engine switchover with scaled EVPN configuration. [PR1401669](#)
- The rpd crashes due to memory corruption in EVPN. [PR1404351](#)
- EVPN database and bridge MAC-table are out of sync due to the interface's flap. [PR1404857](#)
- EVPN routes might show **Route Label: 0** in addition to the real label. [PR1405695](#)
- The rpd might crash after NSR switchover in an EVPN scenario. [PR1408749](#)
- Local L2ALD proxy MAC+IP advertisements accidentally delete MAC+IP EVPN database state from remotely learned type 2 routes. [PR1415277](#)
- The rpd process crash on backup Routing Engine after enabling nonstop-routing with EVPN. [PR1425687](#)
- The device might proxy the ARP probe packets in an EVPN environment. [PR1427109](#)
- IP is missing in mac-ip-table of EVPN database but is present in the EVPN database when CE interface has two primary IP address. [PR1428581](#)
- Extra incorrect MAC move might be seen when the host moves continuously between the different ESI. [PR1429821](#)
- Stale MAC addresses are present in the bridge MAC-table in a EVPN/MPLS scenario. [PR1432702](#)
- Configuring ESI on a single-homed 25G port might not work. [PR1438227](#)

Flow-based and Packet-based Processing

- Fragmentation and ALG support for Power Mode IPsec. [PR1397742](#)

Forwarding and Sampling

- The LSI binding for the IPv6 neighbor is missing. [PR1388454](#)
- Firewall flexible match syntax clarification. [PR1389103](#)
- In Junos OS Release 13.3R9.13, the firewall filter action, "decapsulate gre", decapsulates gre, ip-over-ip, and ipv6-over-ip, but in 17.3R3.9, it only decapsulates gre. [PR1398888](#)

General Routing

- In a BGP/MPLS scenario, if the next hop type of label route is indirect, disabling and enabling the **family mpls** of the next hop interface might cause the route to go into a dead state. [PR1242589](#)
- Large-scale user's log in and log out might cause mgd memory leak. [PR1352504](#)
- Packet Forwarding Engine selector get stuck in rerouted state on unilist NH after primary aggregated Ethernet interface is link deactivated and activated. [PR1354786](#)
- The voltage high alarm might not be cleared when the voltage level comes back to normal for a MIC on an MPC5E. [PR1370337](#)
- The filter service might fail to get installed for the subscriber in a scaled BBE scenario. [PR1374248](#)
- In a subscriber scenario, FPC errors might be seen. [PR1380566](#)
- The routes learned over an interface will be marked as "dead" next hop after changing the prefix-length of IPv6 address on that interface. [PR1380600](#)
- Traffic is silently discarded that is caused by FPC offline in a MC-LAG scenario. [PR1381446](#)
- High cpu utilization for chassisd on bsys, approximately 20 percent at steady state. [PR1383335](#)
- Disable reporting of correctable single-bit error on Hybrid Memory Cube (HMC) and prevent Major Alarm. [PR1384435](#)
- Subscriber connection setup is 30 percent lower than expected. [PR1384722](#)
- The rpd might crash when switchover is performed along with configuration changes being committed. [PR1385005](#)
- Incorrect log message for chip errors (extra dash "-"). [PR1385066](#)
- The MPC10E line card interface filter statistics are not showing the input packet count or rejects. The **show pfe statistics traffic** statement does not report for any normal discard. [PR1383579](#)
- The rpd and KRT queue might get stuck in a VRF scenario. [PR1386475](#)

- Behavior of the **set interfaces ams0 service-options session-limit rate <integer value>** has changed. [PR1386956](#)
- Migrate from syslog API to errmsg API - VMhost messages on Junos OS. [PR1387099](#)
- Some SFBs might go down when one of the PSMs in the chassis generates a bad output voltage which is out-of-range. [PR1387737](#)
- IPsec IKE keys are not cleared when delete/clear notification is received. [PR1388290](#)
- BBE SMGD core files are generated if MTU is changed while subscribers are logged in on the physical interface. [PR1389611](#)
- The jnxFruState might show incorrect PIC state after replacing a MPC with another MPC having less PICs. [PR1390016](#)
- Traffic destined to VRRP VIP gets dropped as filter is not updated to related logical interface. [PR1390367](#)
- **Delete chassis redundancy** will not give commit warning. [PR1390575](#)
- The BNG might not respond with PADO and create any Demux interface when PPPoE PADI packet is received. [PR1390989](#)
- The Packet Forwarding Engine might not respond with ICMP time exceeded error when packet arrives from the subscriber. [PR1391932](#)
- FPC might reboot on vMX in a subscriber scenario. [PR1393660](#)
- Junos OS enhancement configuration statement to modify mcontrol watchdog timeout. [PR1393716](#)
- The FPC cards might not come up while performing unified ISSU on MX10003. [PR1393940](#)
- IDS aggregate configuration statement should not be considered for the installation of the IDS dynamic filter [PR1395316](#)
- L3 gateway did not update ARP entries if IP or MAC quickly move from one router to another router in EVPN-VXLAN environment. [PR1395685](#)
- The MPC, and Forwarding Engine Board (AFEB or TFEB) with channelized OC MIC might crash with the generation of core files. [PR1396538](#)
- Adding IRB to bridge-domain with PS interface causes kernel crash. [PR1396772](#)
- Subscriber flapping might cause SMID resident memory leak. [PR1396886](#)
- The routing protocol process (rpd) has facilities to attempt to trap certain classes of nonfatal bugs by continuing to run, but it generates a "soft" core file. [PR1396935](#)
- Seeing **VMHost RE 0 Secure BIOS Version Mismatch** and **VMHost RE 1 Secure Boot Disabled** alarms. [PR1397030](#)
- The service PIC might crash while changing CGNAT mode. [PR1397294](#)
- The **show system firmware** command might provide unexpected output on some MX Series routers such as MX104. [PR1398022](#)

- Wrong transmit clock quality is observed when router is in holdover. [PR1398129](#)
- MPLSoUDP/MPLSoGRE tunnel might not come up on the interface route. [PR1398362](#)
- JET/PRPD incompatibility for the rib_service.proto field RouteGateway.weight from Junos OS Release 18.4R1 to Release 18.4R2 onward. [PR1400563](#)
- The mgd-api might crash due to a memory leak. [PR1400597](#)
- Only one Packet Forwarding Engine could be disabled on FPC with multiple Packet Forwarding Engines in error/wedge condition. [PR1400716](#)
- The **show | compare** command output on global group changes lose the diff context after a rollback or 'load update' is performed. [PR1401505](#)
- The TCP connection between ppmd and ppmn might be dropped due to a kernel issue. [PR1401507](#)
- The FPC generates core files due to a corner case scenario (race condition between RPF, IP flow). [PR1401808](#)
- Traffic loss is seen in IGMP subscribers after GRES. [PR1402342](#)
- The MPC might crash due to the CPU hogging by dfw thread. [PR1402345](#)
- DHCP subscriber cannot reconnect over dynamic VLAN demux interfaces due to RPF check failure. [PR1402674](#)
- Observed rpd core files when few colored LSPs changed to uncolored LSPs. [PR1403208](#)
- The sync_response received earlier for interface sensor subscribed in on-change mode. [PR1403672](#)
- Continuous kernel crashes might be observed in the backup Routing Engine or VC-BM. [PR1404038](#)
- With MS-MPC and MS-MIC service cards, Syslog messages for port block interim might show 0.0.0.0 for the private-IP and PBA release messages might show the NAT'd IP as the private IP. [PR1404089](#)
- The FPC might crash in a CoS scenario. [PR1404325](#)
- The repd continues to generate core files on VC-Bm when there are too many IPv6 addresses on one session. [PR1404358](#)
- Incorrect output of the assigned prefixes to the subscriber in the output of the **show interface < dynamic demux interface>** command. [PR1404369](#)
- On an MX10003 and an MX10008, its i2c bus might fail a read operation. [PR1405787](#)
- MPC might generate core files after restarting the FPC that belongs to targeting aggregate Ethernet and host subscribers. [PR1405876](#)
- NAT64 translation issues of **ICMPv6 Packet Too Big** message with MS-MPC/MS-PIC. [PR1405882](#)
- The FPC crash might be observed in MS-MPC HA environment. [PR1405917](#)
- Fabric performance drops on MPC7, MPC8, and MPC9E and SFB2 based MX2000 routers. [PR1406030](#)
- A rpd crash is seen post configuration commit and bt has pointers on receiving SNMP packet. [PR1406357](#)

- Traffic impact might be seen if auto-bandwidth is configured for RSVP LSPs. [PR1406822](#)
- New CLI option to display DF and MLR in split format. [PR1406884](#)
- MX10003 gives a cosmetic error message **ALARMD_CONNECTION_FAILURE: after 60 attempts crafted connect returned error: Connection refused**. [PR1406952](#)
- Layer 2 VPN might flap repeatedly after the link up between PE and CE devices. [PR1407345](#)
- The rpd might crash when a commit check is executed on LDP trace options filtering. [PR1407367](#)
- NPC core file is generated after daemon restart in `jnh_get_oif_nh ()` routine. [PR1407765](#)
- Ephemeral database might get stuck during commit. [PR1407924](#)
- Traffic forwarding fails when crossing VCF members. [PR1408058](#)
- **openconfig-network-instance:network-instances** support for IS-IS must be hidden unless supported. [PR1408151](#)
- Group VPN (GVPN): ToS/DSCP byte is not copied into the outer IPSec header during IP header preservation. [PR1408168](#)
- Alarm mismatch in total memory is detected after **reboot vmhost both**. [PR1408480](#)
- The MPC line cards might crash when performing unified ISSU to Junos OS Release 19.1R1 or above. [PR1408558](#)
- Python script might stop working due to **Too many open files** error. [PR1408936](#)
- MX-service templates are not cleaned up. [PR1409398](#)
- MX-MPC2-3D-EQ and MPC-3D-16XGE-SFPP will now show the **Exhaust A** temperature, rather than the Intake temperature. [PR1409406](#)
- MIC-MACSEC-20GE supports Extended Packet Numbering (XPN) mode on 1-Gigabit or 10-Gigabit Ethernet interfaces [PR1409457](#)
- Telemetry: **interface-set meta-data** needs to include the CoS TCP names in order to aid collector reconciliation with queue-stats data. [PR1409625](#)
- The non-existent subscribers might appear at **show system resource-monitor subscribers-limit chassis extensive** output. [PR1409767](#)
- FPC might crash during next hop change when using MPLS inline-jflow. [PR1409807](#)
- MX80 drops DNS responses which contain an underscore. [PR1410062](#)
- When using SFP+, the interface optic output might be non-zero even though the interface has been disabled. [PR1410465](#)
- Traffic loss might be seen on MPC8E or MPC9E after request one of the SFB2s offline/online. [PR1410813](#)
- Kernel replication failure might be seen if an IPv6 route next hop points to an ether-over-atm-llc ATM interface. [PR1411376](#)

- Packet Forwarding Engine heap memory leak might happen during frequent flapping of PPPoE subscribers connected over aggregated Ethernet interface. [PR1411389](#)
- Virtual Route Reflector might report **DAEMON-3-JTASK_SCHED_SLIP_KEVENT** error on some hypervisor or host machine because of NTP sync. Routing protocol might be impacted. [PR1411679](#)
- If GRE over GRE tunnel is used for sending Routing Engine-originating traffic, the traffic cannot be encapsulated properly although the GRE over GRE tunnel works for transit traffic. [PR1411874](#)
- The **file copy** command might not work if the routing-instance option is not specified. [PR1412033](#)
- On MX10003 router, the rpd process crash with switchover-on-routing-crash does not trigger the Routing Engine switchover and the rpd process on the master Routing Engine goes into STOP state. [PR1412322](#)
- Junos OS PCC might reject PCUpdate/PCCreate message if there is metric type other than type 2. [PR1412659](#)
- PPPoE subscribers might not be able to login after unified ISSU. [PR1413004](#)
- The rpd memory leak might be seen due to a wrong processing of a transient event. [PR1413224](#)
- During unified ISSU from Junos OS Release 16.1R4-S11.1 to Junos OS Release 18.2R2-S1.2, CoS GENCFG write failures are observed. [PR1413297](#)
- The support of inet6 filter attribute for ATM interface is broken in the Junos OS Release 17.2R1 and onwards [PR1413663](#)
- DHCP subscribers over HAG might cause core file generation. [PR1413862](#)
- The services load balance might not be effective for AMS if the hash-key under the **forwarding-options** hierarchy is configured. [PR1414109](#)
- FPC crash might be observed if it reaches the heap utilization limit. [PR1414145](#)
- Firewall filters are not getting programmed into Packet Forwarding Engine. [PR1414706](#)
- The user might not enter the configure mode due to mgd is in lockf status. [PR1415042](#)
- PMTU issue IPv4/IPv6 MX does not respond when MTU exceeded for clients terminated on tunnel type interfaces. [PR1415130](#)
- Port speed change and scaled aggregate Ethernet configuration can lead to MQSS errors and subsequent card crash. [PR1415183](#)
- PCE-initiated LSPs get deleted from the PCC if the PCEP session goes down and gets re-established within the configured **delegation-cleanup-timeout** period. [PR1415224](#)
- The bbe-smgd process might have memory leak while running the **show system subscriber-management route route-type <> routing-instance <>** command. [PR1415922](#)
- jdhcpd core file is observed after deletion of the active lease-query configurations. [PR1415990](#)
- BMP type 1 message with extra 24 bytes at end of the message. [PR1416301](#)

- After a GRES on a MX104 some tunnels will fail to pass traffic after a re-key. [PR1417170](#)
- The ECMP fast reroute protection feature might not work on MX5, MX10, MX40, MX80, and MX104 routers. [PR1417186](#)
- An IPv4 packet with a zero checksum might not be translated to IPv6 packet properly under NAT64 scenario. [PR1417215](#)
- With NETCONF the **xmlns** attribute is displayed twice when the RPC **get-arp-table-information** is sent to the router. [PR1417269](#)
- Some subscribers might be offline when doing GRES or daemon restart. [PR1417574](#)
- Observed zero tunnel statistics on the soft-gre tunnel. [PR1417666](#)
- The BGP session might flap after Routing Engine switchover. [PR1417966](#)
- CGNAT with MS-MPC card does not account for AP-P out of port errors or generate a syslog message when this condition is met. [PR1418128](#)
- There is no SNMP trap message generated for jnxHardDiskMissing/jnxHardDiskFailed on MX10003 routers. [PR1418461](#)
- **Clear PRBS statistics** is ineffective on latest build. [PR1418495](#)
- lsp-cleanup-timer is not being honored when lsp-cleanup-timer is configured to be greater than 2147483647. [PR1418937](#)
- PPPoE compliance issue with RFC2516, the MX allows PPPoE session-id 65535. [PR1418960](#)
- A PPP session under negotiation might be terminated if another PPPoE client bearing the same session ID. [PR1419500](#)
- CPU usage on Service PIC might spike while forming an IPsec tunnel under DEP/NAT-T scenario. [PR1419541](#)
- A new tunnel could not be established after changing the NAT mapping IP address until the IPEC SA Clear command is run. [PR1419542](#)
- rtsock_peer_unconsumed_obj_free_int: unable to remove node from list logged extensively. [PR1419647](#)
- A bbe-mibd memory leak is causing daemon crash when having live subscribers and SNMP OIDs query. [PR1419756](#)
- In the scenario where the MX Series router and the peer device both try to bring an IPsec tunnel up, so both sides are acting as an initiator, if the peer side does not answer the MX ISAKMP requests the MX can bring the peer initiated tunnel down. [PR1420293](#)
- On MX Series routers, the PTP phase is aligned but TE/cTE not good. [PR1420809](#)
- The FPC CPU might be hogged if channelized interfaces are configured. [PR1420983](#)
- Failed to reload keyadmin database for `/var/etc/keyadmin.conf`. [PR1421539](#)
- **bbemg_smgd_lock_cli_instance_db** should not log as error messages. [PR1421589](#)

- MX-VC: VCP port reports MTU value 9152 in the ICMP MTU exceeded message while the VCP port MTU is set to 9148. [PR1421629](#)
- RPM syslogs are not getting generated after deactivating the aggregate Ethernet interface. [PR1421934](#)
- Remote gateway address change is not effective on MX150 router when its an initiator. [PR1421977](#)
- The CoS IEEE-802.1 classifier might not get applied when it is configured with service activation on underlying interface. [PR1422542](#)
- On the MX204 router, the number of PICs per FPC is incorrectly used as 8, that causes MAC allocation failure on the physical interfaces. [PR1422679](#)
- Added support for SFP-T with QSA adapter in MX10003. [PR1422808](#)
- Incorrect PIC mode on MX10003 MX1RU when pic mode is changed to default mode. [PR1423215](#)
- While committing huge configuration customer is seeing the **error: mustd trace init failed** error. [PR1423229](#)
- MX10003: **enhanced-hash-key symmetric** is not effective and not shown on FPC. [PR1423288](#)
- Traffic is dropped after FPC reboot with aggregated Ethernet member links deactivated by the remote device. [PR1423707](#)
- The MPC10 line card crash is seen on Ktree alloc (jnh_dfw_instance_add (filter_index=< optimized out>)) at `../../../../src/pfe/common/applications/dfw/dfw_iff.c:1030 with inline + scale prefix filter`. [PR1423709](#)
- On MX204 optics, "SFP-1GE-FE-E-T" I2C read errors are seen when an SFP-T is inserted into a disabled state port. [PR1423858](#)
- The bbe-smgd process might crash after executing the **show system subscriber-management route prefix <>** command. [PR1424054](#)
- MX10000 port configured for 1-Gigabit flaps after a Routing Engine switchover. [PR1424120](#)
- The interface configured with 1-Gigabit speed on JNP10K-LC2101 cannot come up. [PR1424125](#)
- mgd-api core file is seen while running the gNMI set operation. [PR1424128](#)
- Continuous MAC change might cause CPU hogs and FPC reboot. [PR1424653](#)
- [vMX]Continuous disk error logs on vCP Console (Requesting switchover due to disk failure on ada1). [PR1424771](#)
- The jdhcpd might consume 100 percent CPU and then crash if **dhcp-security** is configured. [PR1425206](#)
- The rpd might crash continuously when MD5 authentication on any protocols is used along with master password. [PR1425231](#)
- Soft-gre tunnel route is lost after reboot or GRES or upgrade in WAG scenario. [PR1425237](#)
- Log messages are seen continuously on MX204 router **fru_is_present: out of range slot 0 for**. [PR1425411](#)
- All interfaces creation fails after NSSU. [PR1425716](#)
- Sometimes, the interface is down after rebooting. [PR1426349](#)

- Traffic loss might be seen when multiple IPsec tunnels are established with the remote peer. [PR1426975](#)
- Traffic is not flowing through MACsec interfaces when configured with an unknown cipher algorithm and change back. [PR1427294](#)
- Execution of the **clear-session re-cli** command should not be allowed from Standby DUT. [PR1428353](#)
- The subscriber IP route might get stuck in bbe-smgd if the subscriber IP address is the same with local IP address. [PR1428428](#)
- Incorrect normalization on routing instance where an interface includes a **vlan-id-range**. [PR1428623](#)
- PTSP subscriber is stuck in configured state. Auto-clear-timer does not work as well. [PR1428688](#)
- Incorrect IGMP statistics for dynamic PPP interfaces are observed. [PR1428822](#)
- L2TP subscriber and MPLS Pseudowire Subscriber volume accounting statistics value remains unchanged post unified ISSU. [PR1429692](#)
- The rpsd daemon is not getting killed on when unconfigured simultaneous to toggling rpd 'force-64-bit', rpsd core file is seen 10 minutes later. [PR1429770](#)
- **Cmerror Op set** log message is missing for **bringup jspec** command-based error simulation in EVO. [PR1430300](#)
- Configuration is prevented from being applied on MX Series routers in subscriber scenario. [PR1430360](#)
- Destination unreachable counter is counting up without receiving traffic. [PR1431384](#)
- The bbe-smgd process might crash if PPPoE subscribers are trying to log in when commit is in progress. [PR1431459](#)
- MX10003 - PEM not present alarm is raised when minimum required PEM exist in the system. [PR1431926](#)
- Error message for **show system resource-monitor** and **show system resource-cleanup** is **error: command is not valid on the qfx5220-32cd**. [PR1435136](#)
- A unified ISSU fails from Junos OS Release 19.1R1 legacy Junos OS release images. [PR1438144](#)

Infrastructure

- SNMP OID IFOutDiscards is not updated when drops increase. [PR1411303](#)
- Increase in Junos image size for Junos OS Release 19.1R1. [PR1423139](#)

Interfaces and Chassis

- LFM sessions might flap during unified ISSU. [PR1377761](#)
- Changing the value of **mac-table-size** to default might lead all FPC to reboot. [PR1386768](#)

- The dcd memory leak might be seen when committing configuration change on static route tag. [PR1391323](#)
- The dcd crash might be seen after deleting the sub interface from VPLS routing-instance and mesh-group. [PR1395620](#)
- NPC crashes at `rt_nh_install (rnh=0x618123d8, rnh_src=0x0, rt=< optimized out>, p_rtt=0x74f886c0)` at `../../../../src/pfe/common/pfe-arch/trinity/applications/route/rt_nh.c:631`. [PR1396540](#)
- Static demux0 logical interfaces do not come up after a configuration change if the underlying interface is et. [PR1401026](#)
- Certain otn-options cause interface flapping during commit. [PR1402122](#)
- Missing mandatory ICCP configuration statement **redundancy-group-id-list** produces misleading error message. [PR1402606](#)
- The subscriber might not be able to access the device due to the conflicted assigned address. [PR1405055](#)
- On MX Series routers, the EX-SFP-1FE-LX SFP transceiver does not initialize with MIC-3D-20GE-SFP-E(EH). [PR1405271](#)
- The cfmd might fail to start after it is restarted. [PR1406165](#)
- The **aaa-options** configuration statement for PPPoE subscribers does not work on the MX80 and MX104 routers. [PR1410079](#)
- OAM CFM MEP flaps might occur when hardware-assisted keep alives are enabled. [PR1417707](#)
- **Monitor Ethernet loss-measurement** command returns Invalid ETH-LM request for unsupported outgoing logical interface. [PR1420514](#)
- Incorrect value on speed will cause traffic destined to the IRB's VIP to be dropped. [PR1421857](#)
- The syslog message **/kernel: %KERN-3: pointchange for flag 04000000 not supported on IFD aex** is seen on executing LFM related configuration commit on the aggregated Ethernet interfaces. [PR1423586](#)
- [EVPN] Aggregate Ethernet interface flaps followed by commit. [PR1425339](#)
- **flexible-queuing-mode** is not working on MPC5E of Virtual Chassis member1. [PR1425414](#)
- PEMs lose DC output power load sharing after PEM switch off and on operation on MX routers. [PR1426350](#)
- CFM message flooding. [PR1427868](#)
- Vrrpd crashes during group mastership change if preemption is configured and logical interface was enabled/activated some time after disabling/deactivation. [PR1429906](#)

Layer 2 Features

- The unicast traffic from IRB interface towards LSI might be dropped due to Packet Forwarding Engine mismatch at egress processing. [PR1381580](#)
- Traffic loss might be seen over LDP-VPLS scenario. [PR1415522](#)
- The rpd crashes after iw0 interface is configured under a VPLS instance. [PR1406472](#)
- In a Layer 2 domain, there might be unexpected flooding of unicast traffic at every 32-40 seconds interval towards all local CE-facing interface. [PR1406807](#)
- Broadcast traffics might be discarded in a VPLS local-switching scenario. [PR1416228](#)
- Commit error will be seen but the commit is processed if adding more than one site under **protocols vpls** in the VPLS routing-instances. [PR1420082](#)

Layer 2 Ethernet Services

- The SNMP query on LACP interface might lead to lacpd crash. [PR1391545](#)
- Log messages **dot1xd[]: task_connect: task ESP CLIENT:....: Connection refused** might be reported in Junos OS Release 17.4 or later. [PR1407775](#)
- DMAC problem of IRB interface for traffic over the Layer 2 circuit. [PR1410970](#)
- The IRB interface might flap after committing configuration change on any interface. [PR1415284](#)
- The IPv6 neighbor might become unreachable after the primary link goes down in a VPLS scenario. [PR1417209](#)
- The jdhcpd becomes aware about some of the existing configuration only after 'commit full' or jdhcpd restart. [PR1419437](#)
- Change the nd6 next hops to reject NH once Layer 2 interfaces gets disassociated with IPv6 entries. [PR1419809](#)
- The jdhcpd process might consistently run at 100 percent CPU and not provide service if **delay-offer** is configured for the DHCP local server. [PR1419816](#)
- JDI-RCT:BBE:DHCP subscribers on non-default routing instance went down after unified ISSU. [PR1420982](#)
- The jdhcpd daemon might crash during continuous stress test. [PR1421569](#)

MPLS

- Not found number of ingress, transit, and egress LSP's as expected. [PR1242558](#)
- Collecting LDP statistics do not work correctly and kernel memory leak is observed after configuring **ldp traffic-statistics**. [PR1258308](#)

- With an SR-TE path with "0" explicit NULL as the innermost label, SR-TE path does not get installed with label "0". [PR1287354](#)
- A RSVP-signaled LSP might stay in down state after a link in the path flaps. [PR1384929](#)
- The rpd process might crash when executing **traceroute mpls bgp**. [PR1399484](#)
- MPLS LSP traffic loss might be seen under rare conditions if CSPF is enabled. [PR1402382](#)
- Scaled MPLS labels might cause slow labels allocation and high CPU utilization. [PR1405033](#)
- The Layer 2 circuit information is not advertised over the LDP session if **ldp dual-transport inet-lsr-id** is different from the router-id. [PR1405359](#)
- Resources might be reserved for stale RSVP LSP when RSVP is disabled on the interface. [PR1410972](#)
- The rpd might crash in BGP-LU with egress-protection while committing configuration changes. [PR1412829](#)
- The rpd might crash if **longest-match** is configured for LDP. [PR1413231](#)
- LDP route is not present in inet6.3 if IPv6 interface address is not configured. [PR1414965](#)
- Rpd memory might leak when RSVP LSP is cleared/re-signaled. [PR1415774](#)
- RSVP signalled LSP takes 3 - 4 minutes before LSP switchover begins, causing long traffic to be silently discarded. [PR1416487](#)
- LDP route might be missing in inet.3 when enabling **sr-mapping-client** on LDP-SR stitching node. [PR1416516](#)
- Traffic might be dropped because of the LDP label corruption after Routing Engine switchover. [PR1420103](#)
- Bad length for Sub-TLV 34 (RFC 8287) in MPLS echo request. [PR1422093](#)
- LDP route metric might not match IGP route metric even with **ldp track-igp-metric** configured. [PR1422645](#)
- Bypass dynamic RSVP LSP tears down too soon when being used for protecting LDP LSP with **dynamic-rsvp-lsp** statement. [PR1425824](#)
- MPLS ping sweep stops working and gets CLI irresponsive. [PR1426016](#)
- When MBB for P2MP LSP fails, it is stuck in the old path. [PR1429114](#)

Network Management and Monitoring

- The chassisd might crash and restart after the AGENTX session timeout between master(snmpd) and sub-agent. [PR1396967](#)
- The snmp query might not get data in scaled L2 circuit environment. [PR1413352](#)
- Syslog filtering(match "regular-expression" statement) does not work if each line of **/etc/syslog.conf** is over 2048 bytes. [PR1418705](#)

Platform and Infrastructure

- The kernel and ksyncd core after dual cb flap at `rt_nhfind_params: rt_nhfind()` found an nh different from that onmaster 30326. [PR1372875](#)
- Traffic is being dropped when passing through MS-DPC to MPC. [PR1390541](#)
- All FPCs might restart after the Layer 3 VPN routes churn multiple times. [PR1398502](#)
- MAP-E some ICMP types cannot be encapsulated or decapsulated on the SI interface. [PR1404239](#)
- Abnormal queue-depth counters are seen in the **show interface queue** command output on interfaces that are associated to XM2 and 3. [PR1406848](#)
- IPv6 traffic might be dropped between VXLAN bridge-domain and IP/MPLS network. [PR1407200](#)
- CoS configuration changes might lead to traffic drop on cascade port in a Junos Fusion setup. [PR1408159](#)
- Traffic is getting dropped when there is a combination of DPC/FPC card and MPC card on egress PE router in Layer 3 VPN. [PR1409523](#)
- The VLAN tag is wrongly inserted on the access interface if the packet is sent from an IRB interface. [PR1411456](#)
- The MPC might crash when one MIC is pulled out while the MIC is booting up. [PR1414816](#)
- Distributed multicast forwarding to the subscriber interface might not work. [PR1416415](#)
- The **op url** command cannot run a script with libs from `/config/scripts`. [PR1420976](#)
- arp request is not replied although **proxy-arp** is configured. [PR1422148](#)
- **show jnh trap-info** with incorrect LU instance crashes and generates a core file on FPC. [PR1423508](#)
- The native VLAN ID of packets might fail to be removed when leaving out. [PR1424174](#)
- The policer bandwidth might be incorrect for the aggregated Ethernet interface after activating the **shared-bandwidth-policer** statement. [PR1427936](#)
- Pre-fragmented ICMP IPv4 packets might fail to arrive at the destination. [PR1432506](#)
- Enable sensor `/junos/system/linecard/qmon/` causing continuous **ppe_error_interrupt** errors. [PR1434198](#)

Routing Policy and Firewall Filters

- The rpd process might crash when the policy configuration is being changed. [PR1357802](#)
- MX-Series: The CLI statement **as-path-expand last-as** causes commit failures. [PR1388159](#)
- The rpd process might crash when **routing-options flow** configuration is removed. [PR1409672](#)

Routing Protocols

- Dynamic NextHop template cache does not shrink when application frees the NextHop template. [PR1346984](#)
- Qualified next hop of static route might not be withdrawn when BFD is down. [PR1367424](#)
- The static route might persist even after its BFD session goes down. [PR1385380](#)
- BGP sessions might keep flapping on backup RE if proxy-macip-advertisement is configured on IRB interface for EVPN-VXLAN. [PR1387720](#)
- In rare cases, rpd process might crash after Routing Engine switchover when BGP multipath and L3VPN **vrf-table-label** are configured [PR1389337](#)
- BGP IPv6 routes with IPv4 next hop causes a rpd crash. [PR1389557](#)
- Multicast traffic might be interrupted in some H-VPLS scenario. [PR1394213](#)
- BGP DMZ LINK BANDWIDTH - not able to aggregate bandwidth, when applying the policy. [PR1398000](#)
- The process rpd might crash in a BGP setup with NSR enabled. [PR1398700](#)
- Unexpectedly high packet loss might be observed after an uplink failure when the MoFRR feature is used in a scaled environment. [PR1399457](#)
- There might be unexpected packets drop in MoFRR scenario if active RPF path is disabled. [PR1401802](#)
- The rpd might be stuck at 100 percent when **auto-export** and **BGP add-path** are configured. [PR1402140](#)
- BGP router on the same broadcast subnet with its neighbors might cause IPv6 routing issue on the neighbor from other vendors. [PR1402255](#)
- Some times when a new logical router is configured, the logical router core might be seen on the system. [PR1403087](#)
- Memory leaks when labeled-isis transit routes is created as a chain composite next hop. [PR1404134](#)
- Extended traffic loss might be seen after link recovery when **source-packet-routing** is used on OSPF P2P links. [PR1406440](#)
- SBFD failure is seen with a special IP address like 127.0.0.1 under interface lo0. [PR1406631](#)
- IGMP join through PPPOE sub is not propagated to upstream PIM. [PR1407202](#)
- The rpd crashes on static route configuration for multicast source. [PR1408443](#)
- On MX Series routers, mcsnoopd core file is generated immediately after the commit change related to EVPN-VXLAN configuration. [PR1408812](#)
- SID label operation might be performed incorrectly in an OSPF SPRING environment. [PR1413292](#)
- An unexpected AS prepending action for AS path might be seen after the **no-attrset** statement is configured or deleted with vrf-import/vrf-export configuration. [PR1413686](#)
- The CPU utilization of the rpd process is stuck at 100 percent if BGP multipath is configured. [PR1414021](#)

- Dynamic routing protocol flaps with vmhost Routing Engine switchover on Next Generation-Routing Engine. [PR1415077](#)
- The IS-IS SR route sent by the mapping server might be broken for ECMP. [PR1415599](#)
- Route info might be inconsistent between RIB and OSPF database when using the OSPF LFA feature. [PR1416720](#)
- A memory leak in rpd might be seen if source packet routing is enabled for the IS-IS protocol. [PR1419800](#)
- IPv6 IS-IS routes might be deleted and not be reinstalled when MTU is changed under the logical interface level for family inet6. [PR1420776](#)
- A timing issue is seen while closing a PIM task and an auto-RP at the same time that might sometimes result in an rpd core file generation. [PR1426711](#)
- The rpd might crash while handling the withdrawal of an imported VRF route. [PR1427147](#)
- The rpd process might crash with OSPF overload as external configuration. [PR1429765](#)
- The **request system core-dump routing** CLI is not supported in cRPD. [PR1433349](#)

Services Applications

- Hide HA information when the service set does not have HA configured. [PR1383898](#)
- The following log message is seen: **SPD_CONN_OPEN_FAILURE: spd_svc_set_summary_query: unable to open connection to si-0/0/0 (No route to host)**. [PR1397259](#)
- Inconsistent content might be observed to the access line information between ICRQ and PPPoE. message [PR1404259](#)
- The stale si- logical interface might be seen when L2TP subscribers with duplicated prefixes or framed-route log in. [PR1406179](#)
- The kmd process might crash on MX/ACX platforms when IKEv2 is used. [PR1408974](#)
- The ERA value does not match with configured values while verifying if the new ERA settings are reflected in messages log. [PR1410783](#)
- The jpppd generates core files on LNS. [PR1414092](#)
- L2TP LAC might fail to tunnel static pp0 subscriber to the desired LNS. [PR1416016](#)
- IPsec SA might not come up when the local gateway address is a VIP for a VRRP configured. interface. [PR1422171](#)
- In subscriber with L2TP scenario, subscribers are stuck in INIT state forever. [PR1425919](#)
- Some problems might be seen if client negotiates LCP with no ppp-options to LAC. [PR1426164](#)

Software Installation and Upgrade

- The configuration loss and traffic loss might be seen if the backup Routing Engine is zeroized and is then switched over to master within short time. [PR1389268](#)
- JSU might be deactivated from FPC in case of power cycle. [PR1429392](#)

Subscriber Access Management

- The DHCPv6-PD client connection might be terminated after commit when the RADIUS assigned address is not defined within the range of a local pool. [PR1401839](#)
- The authd crash might be seen due to a memory corruption issue. [PR1402012](#)
- Adding a firewall filter service through the **test aaa** command causes a crash in dfwd. [PR1402051](#)
- The authd re-uses address too quickly before jdhcpd completely cleans up the old subscriber that is causing the flooding error **log DH_SVC_DUPLICATE_IPADDR_ERR: Failed to add x.x.x.x as it is already used by xxx**. [PR1402653](#)
- Continuous log message **authd[18454]: %DAEMON-3-LI: liPollTimerExpired returned 0**. [PR1407923](#)
- Authd telemetry: Linked pool head attribute is incorrect for single pools. [PR1413293](#)
- CoA-NACK is not sent when performing negative COA request tests by sending incorrect session-id. [PR1418144](#)
- Subscribers might not be able to re-login in Gx-plus provisioning scenario. [PR1418579](#)
- PPPoE session might be disconnected when LI attributes are received in access-accept with invalid data. [PR1418601](#)
- Address allocation issue with linked pools when using linked-pool-aggregation. [PR1426244](#)
- RADIUS authentication server might always be marked as DEAD. [PR1429528](#)

User Interface and Configuration

- The **show configuration** and **rollback compare** commands are causing high CPU usage. [PR1407848](#)
- Commit reject occurs for ae0.0 vlan-id-list and routing-instance vlan-id (but does not reject for vlan-range). [PR1427278](#)

VPNs

- The receivers belonging to a routing instance might not receive multicast traffic in an Extranet next-generation MVPN scenario. [PR1372613](#)
- Downstream interface is not removed from multicast route after getting PIM prune. [PR1398458](#)

- Routes with multiple communities are being rejected in an inter-AS next-generation MVPN scenario. [PR1405182](#)
- For rosen MVPN configuration with data-mdt, the **show pim mdt data-mdt-limit instance < instance name>** CLI command with family option causes high CPU usage of the rpd. [PR1405887](#)
- The rpd might crash in rosen MVPN scenario when the same provider tunnel source address is being used for both IPv4 and IPv6. [PR1416243](#)
- The deletion of (S,G) entry might be skipped after the PIM join timeout. [PR1417344](#)
- The rpd process might crash in rare conditions when Extranet next-generation MVPN is configured. [PR1419891](#)
- A permanent traffic loss is seen on next-generation MVPN selective tunnels after Routing Engine switchover (one-time). [PR1420006](#)
- The rpd process might crash and core file is generated during **mpls ping** command on L2 circuit. [PR1425828](#)

SEE ALSO

[What's New | 76](#)

[What's Changed | 96](#)

[Known Limitations | 100](#)

[Open Issues | 102](#)

[Documentation Updates | 129](#)

[Migration, Upgrade, and Downgrade Instructions | 130](#)

[Product Compatibility | 137](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.2R1 documentation for MX Series.

SEE ALSO

[What's New | 76](#)

[What's Changed | 96](#)

[Known Limitations | 100](#)

[Open Issues | 102](#)
[Resolved Issues | 111](#)
[Migration, Upgrade, and Downgrade Instructions | 130](#)
[Product Compatibility | 137](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 19.2 | 131](#)
- [Procedure to Upgrade to FreeBSD 11.x based Junos OS | 131](#)
- [Procedure to Upgrade to FreeBSD 6.x based Junos OS | 133](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 135](#)
- [Upgrading a Router with Redundant Routing Engines | 136](#)
- [Downgrading from Release 19.2 | 136](#)

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the MX Series. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

Starting in Junos OS 18.3R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

The following table shows detailed information about which Junos OS can be used on which products:

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 11.x-based Junos OS
MX5,MX10, MX40,MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 19.2

NOTE: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful.

Issue the following command:

```
user@host> request system snapshot
```

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the **juniper.conf** and **ssh** files) might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the [Installation and Upgrade Guide](#).

For more information about the installation process, see [Installation and Upgrade Guide](#) and [Upgrading Junos OS with Upgraded FreeBSD](#).

Procedure to Upgrade to FreeBSD 11.x based Junos OS

Products impacted: MX240, MX480, MX960, MX2010, and MX2020.

To download and install FreeBSD 11.x based Junos OS:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.

7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the routing platform.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

All customers except the customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-19.2R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-19.2R1.9-signed.tgz
```

Customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos package):

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-32-19.2R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot
source/junos-install-mx-x86-64-19.2R1.9-limited.tgz
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
 - **ftp://hostname/pathname**

- `http://hostname/pathname`
- `scp://hostname/pathname`

Do not use the **validate** option while upgrading from Junos OS (FreeBSD 6.x) to Junos OS (FreeBSD 11.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 11.x, and Junos OS (FreeBSD 6.x) would not be able to run these programs. You must run the **no-validate** option. The **no-validate** statement disables the validation procedure and allows you to use an import policy instead.

Use the **reboot** command to reboot the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).

NOTE: After you install a Junos OS Release 19.2 **jinstall** package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add no-validate** command and specify the **jinstall** package that corresponds to the previously installed software.

NOTE: Most of the existing **request system** commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the [Installation and Upgrade Guide](#).

Procedure to Upgrade to FreeBSD 6.x based Junos OS

Products impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.x based Junos OS:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the routing platform.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

- All customers except the customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

```
user@host> request system software add validate reboot source/jinstall-ppc-19.2R1.9-signed.tgz
```

- Customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos OS package):

```
user@host> request system software add validate reboot  
source/jinstall-ppc-19.2R1.9-limited-signed.tgz
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.

- For software packages that are downloaded and installed from a remote location:

- `ftp://hostname/pathname`
- `http://hostname/pathname`
- `scp://hostname/pathname`

The **validate** option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Use the **reboot** command to reboot the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 19.2 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2, and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform the following Junos OS installation on each Routing Engine separately to avoid disrupting network operation:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine, and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the [Installation and Upgrade Guide](#).

Downgrading from Release 19.2

To downgrade from Release 19.2 to another supported release, follow the procedure for upgrading, but replace the 19.2 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

SEE ALSO

What's New 76
What's Changed 96
Known Limitations 100
Open Issues 102
Resolved Issues 111
Documentation Updates 129
Product Compatibility 137

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 137](#)

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on MX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

[What's New | 76](#)

[What's Changed | 96](#)

[Known Limitations | 100](#)

[Open Issues | 102](#)

[Resolved Issues | 111](#)

[Documentation Updates | 129](#)

[Migration, Upgrade, and Downgrade Instructions | 130](#)

Junos OS Release Notes for NFX Series

IN THIS SECTION

- New and Changed Features | 138
- Changes in Behavior and Syntax | 140
- Known Behavior | 141
- Known Issues | 143
- Resolved Issues | 146
- Documentation Updates | 147
- Migration, Upgrade, and Downgrade Instructions | 147
- Product Compatibility | 150

These release notes accompany Junos OS Release 19.2R1 for the NFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os

New and Changed Features

IN THIS SECTION

- Architecture | 139
- Application Security | 139
- Virtual Network Functions | 139

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for NFX Series devices.

Architecture

- **Open vSwitch (OVS) integrated with Data Plane Development Kit (DPDK)**—Starting in Junos OS Release 19.2R1, NFX150-S1 and NFX150-S1E devices support OVS integrated with DPDK that offers better network packet throughput and lower latencies.

[See [Benefits and Uses of NFX150](#).]

Application Security

- **Application-based multipath support (NFX Series)**—Starting in Junos OS Release 19.2R1, application-based multipath routing is supported on NFX150 devices.

Multipath routing allows the sending device to create copies of packets, send each copy through two or more WAN links. On the other end, multipath calculates the jitter and packet loss for the combined links and estimates the jitter and packet loss for the same traffic on individual links. You can compare the reduction in packet loss when combined links instead of individual links are used. Sending multiple copies of traffic ensures timely delivery of the sensitive application traffic.

Multipath support in SD-WAN uses case enhances application experience.

[See [Application Quality of Experience](#).]

- **Application-level logging for AppQoE (NFX Series)**—Starting in Junos OS Release 19.2R1, NFX series devices support application-level logging for AppQoE. This feature reduces the impact on the CSO or log collector device while processing a large number of system log messages generated at the session-level. The device maintains session-level information and provides system log messages for the session level. Replacing session-level logging with application-level logging decreases the overhead on the device and increases AppQoE throughput.

[See [AppQoE](#).]

Virtual Network Functions

- **Disable VNF interfaces (NFX150 and NFX250 NextGen)**—Starting in Junos OS Release 19.2R1, you can manually disable the VNF interfaces (eth0 through eth9) on the OVS or custom bridge on NFX150 and NFX250 NextGen devices.

[See [Configuring VNF Interfaces and VLANs](#).]

- **MAC flooding on VNF interfaces (NFX150 and NFX250 NextGen)**—Starting in Junos OS Release 19.2R1, changes to the default MAC flooding behavior of the virtualized network function (VNF) interfaces improve the performance of multicast traffic. If a VNF interface is not attached to a VLAN, drop flow is not configured. The interface functions as a trunk port that can receive and forward the VLAN traffic.

In earlier releases, if a VNF interface is not attached to a VLAN, drop flow is configured and the VNF interface drops the outgoing traffic.

[See [Configuring VNF Interfaces and VLANs.](#)]

- **Bootstrap configuration of a VNF using a config-drive (NFX150 and NFX250 NextGen)**—Starting in Junos OS Release 19.2R1, you can bootstrap a VNF using an attached config drive that contains a bootstrap-config ISO file on NFX150 and NFX250 NextGen devices. The config drive is a virtual drive, which can be a CD-ROM, USB drive or Disk drive associated to a VNF with the configuration data. Configuration data can be files or folders, which are bundled in the ISO file that makes a virtual CD-ROM, USB drive, or Disk drive.

[See [Preparing the Bootstrap Configuration on NFX150 Devices.](#)]

[See [Preparing the Bootstrap Configuration on NFX250 NextGen Devices.](#)]

SEE ALSO

[What's Changed | 140](#)

[Known Limitations | 141](#)

[Open Issues | 143](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Migration, Upgrade, and Downgrade Instructions | 147](#)

[Product Compatibility | 150](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Factory-default Configuration | 141](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the NFX Series devices.

Factory-default Configuration

- **Plug-and-play configuration (NFX150 and NFX250 NextGen devices)**—Starting in Junos OS Release 19.2R1, the factory default configuration is modified to include the secure router plug-and-play configuration.

SEE ALSO

[What's New | 138](#)

[Known Limitations | 141](#)

[Open Issues | 143](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Migration, Upgrade, and Downgrade Instructions | 147](#)

[Product Compatibility | 150](#)

Known Behavior

IN THIS SECTION

• [Interfaces | 141](#)

• [Platform and Infrastructure | 142](#)

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the NFX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Interfaces

- On NFX250 devcies, the maximum number of VLAN interfaces on the OVS that can be configured in the system is limited to 20. [PR1281134](#)

- On NFX150 devices, the TCP and ICMP RPM probes take the best-effort queue of the outgoing interface, instead of the network control queue. As a workaround, configure a DSCP value such as nc1 for the RPM probes to take the network control queue. [PR1329643](#)
- On NFX150 devices, the PPPoE session does not come up on the interface due to the hardware limitation for both tagged and untagged cases. As a workaround, enable the promiscuous mode on the interface. [PR1347830](#)

Platform and Infrastructure

- The Routing Engine boots from the secondary disk when you:
 - Press the reset button on the RCB front panel, while the RE is booting up before Junos OS reboots.
 - Upgrade the software by booting from the network using the **request vmhost reboot network** command, and the system fails to boot from the network.
 - Upgrade the BIOS and it fails.
 - Reboot the system and it hangs before Junos OS reboots.

As a workaround, interrupt the boot process to select the primary disk. [PR1344342](#)

- Starting in Junos OS Release 18.4, NFX150 devices support two versions of disk layout. In the older version of the disk layout, you could upgrade or downgrade from Junos OS Release 18.4. With the new disk layout, a downgrade to releases later than Junos OS Release 18.4 is not possible. As a workaround, avoid operations that reformat the disk layout. [PR1379983](#)

SEE ALSO

[What's New | 138](#)

[What's Changed | 140](#)

[Open Issues | 143](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Migration, Upgrade, and Downgrade Instructions | 147](#)

[Product Compatibility | 150](#)

Known Issues

IN THIS SECTION

- [High Availability | 143](#)
- [Interfaces | 143](#)
- [Platform and Infrastructure | 144](#)
- [Routing Protocols | 145](#)
- [Virtual Network Functions \(VNFs\) | 145](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for the NFX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

High Availability

- On an NFX150 high availability chassis cluster, the host logs updated in the system log messages might not show the correct time stamp. As a workaround, convert the UTC time stamp to local time zone. [PR1394778](#)

Interfaces

- When you run the **show chassis fpc** or **show chassis fpc details** command, the **Temperature** field in the command output message is displayed as **Testing**. [PR1433221](#)
- On NFX150 and NFX250 NextGen devices, the **link disable** option puts the analyzer interface in inconsistent state with the link state as **down** and admin state as **up**. [PR1442224](#)
- On NFX150 and NFX250 NextGen devices, while configuring vmhost vlans using vlan-id-list, system allows duplicate vlan-ids in the vlan-id-list. [PR1438907](#)
- On NFX Series devices, ping does not work between the cross-connected interfaces configured with **interface deny-forwarding** option. [PR1442173](#)
- On NFX150 and NFX250 NextGen devices, cross-connect stays down even if all linked interfaces are up. [PR1443465](#)
- On NFX250 devices, if the IRB interface configuration and DHCP service configuration on JDM are removed and rolled back while retaining the VLAN mapping to the IRB interface, the DHCP service fails

to assign IP address to the corresponding VNF interfaces and the service chaining fails. As a workaround, remove the VLAN mapping to the IRB interface along with IRB and DHCP service configuration on JDM. [PR1234055](#)

- On an NFX250 NextGen device, you cannot configure more than 93 logical interfaces. An error message **dcf_ng_ifl_alloc_hw_token: Hardware token exhausted-IFL and DCD_CONFIG_WRITE_FAILED with no buffer space available** is logged in the log messages. [PR1424180](#)
- Starting in Junos OS Release 19.2R1, when you transition NFX150 devices from PPPoE configuration to non-PPPoE configuration in a non-promiscuous mode, the interface hangs without any traffic flow. [PR1409475](#)
- On NFX150 devices, only the CFM cells that are configured for MEP levels are exchanged across xDSL MEP. Other MEP level CFM packets are dropped, whereas for Ethernet All MD level along with above level will be exchanged. [PR1409576](#)
- When you issue a **show interface** command on NFX150 devices to check the interface details, the system will not check whether the interface name provided is valid or invalid. The system will not generate an error message if the interface name is invalid. [PR1306191](#)
- When a DHCP server assigns a conflicting IP address to the NFX device interfaces, the NFX device will not send a **DHCP DECLINE** message in response. [PR1398935](#)
- If you plug an unsupported SFP-T transceiver into an NFX150 device and reboot the device, the FPC1 WAN port will not be online. [PR1411851](#)

Platform and Infrastructure

- On NFX150 devices, the **request vmhost reboot in minutes** command with a delay specified in minutes reboots the device immediately. [PR1406018](#)
- On NFX250 devices, the **request load configuration** command output does not match with 18.4 yang. [PR1416106](#)

Routing Protocols

- When there is a static route and an OSPF route is active in the routing table for a specific destination network, a ping initiated to that destination network from the NFX device will fail. [PR1438443](#)

Virtual Network Functions (VNFs)

- On NFX150 and NFX250 NextGen devices, when you add, modify, or delete a VNF interface that is mapped to an L2 or L3 dataplane, the kernel traces might be observed on the NFX device console. [PR1435361](#)
- After you create or delete a VNF on NFX150 and NFX250 NextGen devices, the **request virtual-network-functions console vnf-name** command gives an error that the VNF domain is not found. VNFs are reachable through ssh in this state. [PR1433204](#)
- When you downgrade the software from Junos OS Release 19.2 to Junos OS Release 18.4, the **show virtual-network-functions vnf-name** command does not display the VNF information. [PR1437547](#)
- On NFX150 and NFX250 NextGen devices, if the VNFs are instantiated on Throughput mode, the **sshd** cores are seen and **ssh** to the device may fail rendering the device unreachable and with restricted functionality. Only a power cycle of the device can fix this state. [PR1440285](#)
- On an NFX250-LS1 device operating in Compute mode, the traffic throughput rate will be reduced when the traffic is service chained with a third party VNF with OVS cross-connect configuration. [PR1438687](#)
- On NFX150-S1 devices, configuring the VNF with no-default-interfaces option and disabling the internal management interface (eth0) with the link disable command might not disable the interface. Hence, the liveness status remains alive even if the link is configured to be disabled. [PR1442064](#)
- On NFX150 devices with VNFs configured, when the VNF interfaces are moved from default OVS bridge to custom OVS bridge, there will be duplicate VNF host entries in the `/etc/hosts` file on JDM. [PR1434679](#)

SEE ALSO

[What's New | 138](#)

[What's Changed | 140](#)

[Known Limitations | 141](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Migration, Upgrade, and Downgrade Instructions | 147](#)

[Product Compatibility | 150](#)

Resolved Issues

IN THIS SECTION

- [Interfaces | 146](#)
- [Platform and Infrastructure | 146](#)

This section lists the issues fixed in the Junos OS main release and the maintenance releases for NFX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Interfaces

- On NFX250 devices, an SFP-T interface does not become active when it is plugged into a ge-12/0/0 or a ge-13/0/0 interface. [PR1404756](#)
- On a NFX250 devices with xDSL SFP used on the fiber ports the status of the xDSL SFP was displayed with **Adsl Status** field under cli command **show interfaces int-name**. But whenever a user hot-swaps a xDSL SFP with another xDSL SFP on the same port, then the **Adsl Status** field was not displayed in the **show interfaces** command output. [PR1408597](#)
- On NFX150 devices, FPC0 may not be online after an upgrade and a device reboot is required. [PR1430803](#)

Platform and Infrastructure

- Software upgrade does not delete all images from a previous installation. This occupies about 1GB of storage per upgrade and leads to depletion of storage after several upgrades. [PR1408061](#)
- JDM depends on the libvirtd daemon to manage the guest VM through cli. The libvirtd daemon was stuck and vjunos VM start up failed, which resulted in in-band connectivity issues, the guest VM could not start, and the console was hung. [PR1314945](#)
- The **NFX3/ACX5448:LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified** message is displayed when you commit the configuration on config prompt. As a workaround to exclude this from messages or syslogs, run the **set system syslog user * match "!(LIBCOS_COS_TVP_FC_INFO_NOT_FOUND: Forwarding-class information not specified)** and commit. [PR1376665](#)

SEE ALSO

What's New 138
What's Changed 140
Known Limitations 141
Open Issues 143
Documentation Updates 147
Migration, Upgrade, and Downgrade Instructions 147
Product Compatibility 150

Documentation Updates

There are no errata or changes in Junos OS Release 19.2R1 documentation for NFX Series.

SEE ALSO

What's New 138
What's Changed 140
Known Limitations 141
Open Issues 143
Resolved Issues 146
Migration, Upgrade, and Downgrade Instructions 147
Product Compatibility 150

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 148](#)
- [Basic Procedure for Upgrading to Release 19.2 | 148](#)

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the NFX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information on EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

Basic Procedure for Upgrading to Release 19.2

When upgrading or downgrading Junos OS, use the **jinstall** package. For information about the contents of the **jinstall** package and details of the installation process, see the [Installation and Upgrade Guide](#). Use other packages, such as the **jbundle** package, only when so instructed by a Juniper Networks support representative.

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the device, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the device. For more information, see the [Software Installation and Upgrade Guide](#).

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

To download and install Junos OS Release 19.2R1:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

SEE ALSO

[What's New | 138](#)

[What's Changed | 140](#)

[Known Limitations | 141](#)

[Open Issues | 143](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Product Compatibility | 150](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 150](#)

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on NFX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility Tool](#).

Software Version Compatibility

This section lists the vSRX and Cloud CPE Solution software releases that are compatible with the Junos OS releases on the NFX Series devices.

NOTE: Starting in Junos OS Release 18.1R1, NFX150 and NFX250 devices support the same version of platform software and vSRX. For example, see [Table 1 on page 150](#).

NFX250 Software Version Compatibility

This section lists the vSRX and CloudCPE Solution software releases that are compatible with the Junos OS releases on the NFX250 devices:

Table 1: Software Compatibility Details with vSRX and Cloud CPE Solution

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D40.3	15.1X49-D40.6	Cloud CPE Solution 2.0
15.1X53-D41.6	15.1X49-D40.6	Cloud CPE Solution 2.1

Table 1: Software Compatibility Details with vSRX and Cloud CPE Solution (*continued*)

NFX250 Junos OS Release	vSRX	Cloud CPE Solution
15.1X53-D102.2	15.1X49-D61	Cloud CPE Solution 3.0
15.1X53-D47.4	15.1X49-D100.6	Cloud CPE Solution 3.0.1
15.1X53-D490	15.1X49-D143	Cloud CPE Solution 4.0
15.1X53-D495	15.1X49-D160	Cloud CPE Solution 4.1
15.1X53-D496	15.1X49-D170	Cloud CPE Solution 4.1
15.1X53-D45.3	15.1X49-D61	Not applicable
17.2R1	15.1X49-D78.3	Not applicable
17.3R1	15.1X49-D78.3	Not applicable
17.4R1	15.1X49-D78.3	Not applicable
15.1X53-D471	15.1X49-D143	Not applicable
18.1R1	18.1R1	Not applicable
18.1R2	18.1R2	Not applicable
18.1R3	18.1R3	Not applicable
18.2R1	18.2R1	Not applicable
18.3R1	18.3R1	Not applicable
18.3R2	18.3R2	Not applicable
18.4R1	18.4R1	Not applicable

SEE ALSO

[What's New | 138](#)
[What's Changed | 140](#)

[Known Limitations | 141](#)

[Open Issues | 143](#)

[Resolved Issues | 146](#)

[Documentation Updates | 147](#)

[Migration, Upgrade, and Downgrade Instructions | 147](#)

Junos OS Release Notes for PTX Series Packet Transport Routers

IN THIS SECTION

- [New and Changed Features | 153](#)
- [Changes in Behavior and Syntax | 160](#)
- [Known Behavior | 163](#)
- [Known Issues | 164](#)
- [Resolved Issues | 167](#)
- [Documentation Updates | 170](#)
- [Migration, Upgrade, and Downgrade Instructions | 171](#)
- [Product Compatibility | 175](#)

These release notes accompany Junos OS Release 19.2R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [New and Changed Features: 19.2R1-S4 | 154](#)
- [New and Changed Features: 19.2R1-S1 | 154](#)
- [New and Changed Features: 19.2R1 | 154](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for the PTX Series.

New and Changed Features: 19.2R1-S4

Interfaces and Chassis

- **Support for 1-Gbps on QFX-60S line card on PTX10008 and PTX10016 Routers**—QFX10000-60S-6Q line card supports 1-Gbps speed on its ports (0 to 59). The QFX10000-60S-6Q line card contains 60 SFP+ ports that support 10-Gbps, two dual-speed QSFP28 ports that support either 40-Gbps or 100-Gbps, and four QSFP+ ports that support 40-Gbps. You can individually configure ports 0 to 59 for 10-Gbps or 1-Gbps port speed. Use the **set chassis fpc fps-slot-number pic pic-number port port-number speed 1G** command to change the mode of a port from 10-Gbps to 1-Gbps. The transceivers supported for 1-Gbps are QFX-SFP-1GE-LX, QFX-SFP-1GE-SX, and QFX-SFP-1GE-T.

[See [QFX10000 Line Cards](#) for details on the combination of modes supported on the ports.]

Services Applications

- **Support for Two-Way Active Measurement Protocol (TWAMP) and hardware timestamping of RPM probe messages (MX10000 and PTX10000 routers)**—Starting in Release 19.2R1-S4, Junos OS supports TWAMP and hardware timestamping of RPM probe messages on the MX10008, MX10016, PTX10008 and PTX10016 routers. You can use TWAMP to measure IP performance between two devices in a network. By enabling hardware timestamping of RPM you can account for the latency in the communication of probe messages and also generate more accurate timers in the Packet Forwarding Engine.

[See [Understanding Two-Way Active Measurement Protocol on Routers](#) and [Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX and MX Series Routers](#).]

New and Changed Features: 19.2R1-S1

MPLS

- **Color-based mapping of VPN services over SRTE (PTX Series)**—Starting in Junos OS Release 19.2R1-S1, you can specify a color attribute along with an IP protocol next hop to resolve transport tunnels over static colored and BGP segment routing traffic-engineered (SRTE) label-switched paths (LSPs). This is called the color-IP protocol next hop resolution, where you are required to configure a resolution-map and apply it to the VPN services. Prior to this release, the VPN services were resolved over IP protocol next hops only.

With this feature, you can enable color-based traffic steering of Layer 2 and Layer 3 VPN services.

[See [Color-Based Mapping of VPN Services Overview](#).]

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Hardware

- **Advanced Cooling and Power Components (PTX10000 Routers)**—Starting in Junos OS Release 19.2R1, PTX10000 routers offer 5.5 KW power supplies, new high performance fan trays, and compatible fan tray controllers. The JNP10K-PWR-AC2 power supply supports AC, high-voltage alternating current (HVAC), DC, or high-voltage direct current (HVDC). The JNP10K-PWR-DC2 provides a 5.5 KW upgrade for DC users. The JNP10008-FAN2 and JNP10016-FAN2 offer increased air flow through the chassis. The JNP10008-FAN2 offers 1793 cubic feet per minute (CFM) per fan tray, while the JNP10016-FAN2 provides 3423 CFM per fan tray. Two new fan tray controllers support the new fan trays, the JNP10008-FTC2 and the JNP10016-FTC2.

[See [PTX10016 System Overview](#).]

Interfaces and Chassis

- **Domain Name System (DNS) is VRF aware (PTX Series)**—Starting in Junos OS Release 19.2R1, when the **management-instance** statement is configured at the **[edit system]** hierarchy level, you can use the non-default management routing instance **mgmt_junos** as the routing instance through which the DNS name server is reachable. To specify the routing instance **mgmt_junos**, configure our new configuration statement **routing-instance mgmt_junos**, at the **[edit system name-server server-ip]** hierarchy level.

[See [Management Interface in a Nondefault Instance](#), [Configuring a DNS Name Server for Resolving a Hostname into Addresses](#), [name-server](#), and [show host](#).]

- **Support for health monitoring on the Routing Engine hard disk (PTX10008, PTX1000, PTX5000, and PTX10016)**—Starting in Junos OS Release 19.2R1, you can configure the device to perform certain health checks on the Routing Engine solid-state drive (SSD) and log a health event or raise an alarm in case a predefined health attribute threshold is breached. You can use the **set chassis routing-engine disk smart-check** command to instruct the system to raise an alarm when an SSD health attribute threshold is breached. You can view the alarm by using the command **show chassis alarms**.

[See [smart-check](#).]

Junos Telemetry Interface

- **Sensor- level statistics support on JTI (MX960, MX2008, MX2010, MX2020, PTX5000, PTX1000, and PTX10000 routers and QFX5100 and QFX5200 switches)**—Starting with Junos OS Release 19.2R1, you can issue the Junos operational mode command **show network-agent statistics** to provide more information on a per-sensor level for statistics being streamed to an outside collector by means of remote procedure calls (gRPC) and Junos telemetry interface (JTI). Only sensors exported with gRPC are supported. The command does not support UDP-based sensors.

[See [show network-agent statistics](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **ONCE mode supported using gNMI services and JTI (MX Series, QFX Series, PTX Series)**—Starting in Junos OS Release 19.2R1, you can include the ONCE mode with the **Subscribe** RPC when subscribing

to gRPC Network Management Interface (gNMI) services to export statistics for telemetry monitoring and management using Junos telemetry interface (JTI). ONCE mode ensures that the collector is only streamed telemetry information one time.

The Subscribe RPC and subscription parameters are defined in the [gnmi.proto](#) file.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Packet Forwarding Engine statistics export using gNMI and JTI (PTX1000 and PTX10000 routers)**—Starting in Junos OS Release 19.2R1, you can stream Packet Forwarding Engine statistics to an outside collector using gRPC Management Interface (gNMI) version 0.7.0 and junos telemetry interface (JTI). Before this release, these statistics were exported using OpenConfig gRPC and UDP protocol buffer (gpb) format. OpenConfig gRPC and gNMI are both protocols used to modify and retrieve configurations as well as export telemetry streams from a device in order to manage and monitor it

To provision Packet Forwarding Engine sensors to export data through gNMI, use the Subscribe RPC defined in the [gnmi.proto](#) to specify request parameters.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Specify Routing Instance for JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 19.2R1, you can specify the routing instance to use for remote procedure call (gRPC) services. Include the **routing-instance *instance-name*** at the **[edit system services extension-service request-response grpc]** hierarchy level. The routing instance name specified should match the name of the existing routing instance, such as a name configured under the **[routing-instances]** hierarchy level or **mgmt_junos** if **system management-instance** is configured (the dedicated management routing instance).

Configuring the routing instance lets you choose the VRF for gRPC services. When the routing instance is not configured, the default behavior is that all gRPC-related services are available through the management **fxp0/em0** interface.

MPLS

- **Dynamic creation of segment routing LSPs using BGP protocol next hops (PTX Series)**—Starting in Junos OS Release 19.2R1, you can configure tunnel templates on colored and non-colored segment routing traffic-engineered (SR-TE) paths. These templates enable dynamic creation of segment routing tunnels using protocol next hops with BGP prefixes to resolve destination segment identifiers (SIDs).

With this feature, you can benefit from reduced configuration, especially when the network deployment requires connectivity from each provider edge (PE) device to every other PE device.

[See [Static Segment Routing Label Switched Path](#).]

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (PTX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data model when you include the **action-expand** extension statement in the option or statement definition and reference a script that handles the logic. The **action-expand** statement must include the **script** child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

- **Enhanced sFlow (PTX1000)**—Starting in Junos OS Release 19.2R1, MPLS and GRE traffic flows are added to sFlow functionality for the PTX1000 routers.

[See [Overview of sFlow Technology](#).]

Port Security

- **Fallback PSK for Media Access Control Security (MACsec) (PTX Series)**—Starting in Junos OS Release 19.2R1, fallback PSK for MACsec is supported on PTX Series routers that support MACsec. The fallback PSK provides functionality to establish a secure session in the event that the primary PSKs on each end of a MACsec-secured link do not match.

[See [Configuring Media Access Control Security \(MACsec\) on MX Series Routers](#).]

Routing Policy and Firewall Filters

- **Support for interface, forwarding-class, and loss priority match conditions on egress interfaces (PTX10008, PTX10016)**—Starting with Junos OS Release 19.2R1, you can apply the **interface**, **forwarding-class**, and **loss-priority** firewall filter match conditions in the egress direction on IPv4 and IPv6 interfaces. You configure the match conditions at the **[edit firewall]** hierarchy level. This feature was previously supported in an "X" release of Junos OS.

[See [Firewall Filter Match Conditions and Actions \(QFX10000\)](#).]

Routing Protocols

- **Support for export of BGP Local RIB through BGP Monitoring Protocol (BMP) (PTX Series)**—Starting in Junos OS Release 19.2R1, BMP is enhanced to support monitoring of local RIB (**loc-rib**) policy. The **loc-rib** policy is added to RIB types under the **bmp route-monitoring** statement.

[See: [Understanding the BGP Monitoring Protocol](#).]

Services Applications

- **Support for IPv6 BGP next-hop address in IPv6 and MPLS-IPv6 inline flow record templates (MX Series and PTX Series)**—Starting in Junos OS Release 19.2R1, a new element, IPv6 BGP NextHop Address, is available in the IPv6 inline flow record template and the MPLS-IPv6 inline flow record template to add support for the IPv6 BGP NextHop information element. The new element is supported on both version 9 and version 10 (IPFIX) export formats. The element ID is 63 and the element size is 16 bytes.

[See [Understanding Inline Active Flow Monitoring](#).]

- **Two-Way Active Measurement Protocol (TWAMP) Support (PTX Series)**—Starting in Junos OS Release 19.2R1, PTX Series routers support the Two-Way Active Measurement Protocol (TWAMP). TWAMP defines a standard for measuring IPv4 performance between two devices in a network. You can use the TWAMP-Control protocol to set up performance measurement sessions between a TWAMP client and a TWAMP server, and use the TWAMP-Test protocol to send and receive performance measurement probes..

The destination interface **si-x/y/z** attribute, which is meant for enabling inline services is not supported on PTX Series routers for TWAMP client configurations.

See [Understanding Two-Way Active Measurement Protocol on Routers](#).

Software Defined Networking (SDN)

- **PCE-initiated bypass LSPs (PTX Series)**—Starting in Junos OS Release 19.2R1, the Path Computation Element Protocol (PCEP) functionality is extended to allow a stateful Path Computation Element (PCE) to initiate, provision, and manage bypass label-switched paths (LSPs) for a protected interface. Multiple bypass LSPs with bandwidth reservation can be initiated by the PCE to protect a resource.

With this feature, you can benefit from the LSP state synchronization of manual, dynamic, and PCE-initiated bypass LSPs from a PCE, and leverage on the PCE's global view of the network, resulting in better control over traffic at the time of a failure, and deterministic path computation of protection paths.

[See [Support of the Path Computation Element Protocol for RSVP-TE Overview](#).]

Software Installation and Upgrade

- **The curl binary is packaged and made available on all Junos OS variants (PTX Series)**—The curl binary is a command-line utility, used from the shell, that you can use to perform operations over several transport protocols, including the following: dict, file, ftp, gopher, http, imap, pop3, rtsp, smtp, telnet, tftp. The features enabled on Junos OS are curl version 7.59, libcurl version 7.59.

System Management

- **Support for transferring accounting statistics files and router configuration archives using HTTP URL (PTX Series)**—Starting in Junos OS Release 19.2R1, you can transfer accounting statistics files and router configuration archives to remote servers by using an HTTP URL. In addition to SCP and FTP, the following HTTP URL will be supported under the **archive-sites** statement:

`http://username@host:url-path password password`

- To transfer accounting statistics files, configure **archive-sites** under **[edit accounting-options file <filename>]** hierarchy.
- To transfer router configuration archival, configure **archive-sites** under **edit system archival configuration** hierarchy.
- To view the statistics of transfer attempted, succeeded, and failed, use the **show accounting server statistics archival-transfer** command.
- To clear the statistics of transfer attempted, succeeded, and failed, use the **clear accounting server statistics archival-transfer** command.

[See [archive-sites](#), [Backing Up Configurations to an Archive Site](#), [show accounting server statistics archival-transfer](#), and [clear accounting server statistics archival-transfer](#)].

- **Precision Time Protocol (PTP) transparent clock with IPv6 transport (PTX10001-20C and ACX6360-OR devices)**—Starting with Junos OS Release 19.2R1, PTP using IPv6 transport synchronizes clocks throughout a packet-switched network. With a transparent clock, the PTP packets are updated with residence time as the packets pass through the routers. There is no master clock-slave clock designation. With an end-to-end transparent clock, only the residence time is included. The residence time can be sent in a one-step process, which means that the timestamps are sent in one packet.

You can configure the transparent clock at the **[edit protocols ptp]** hierarchy level.

[See [Understanding Transparent Clocks in Precision Time Protocol.](#)]

SEE ALSO

[What's Changed | 160](#)

[Known Limitations | 163](#)

[Open Issues | 164](#)

[Resolved Issues | 167](#)

[Documentation Updates | 170](#)

[Migration, Upgrade, and Downgrade Instructions | 171](#)

[Product Compatibility | 175](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [What's Changed in Release 19.2R1-S5 | 161](#)
- [What's Changed in Release 19.2R1 | 161](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the PTX Series.

What's Changed in Release 19.2R1-S5

General Routing

- **Logical Interface is created along with physical Interface by default (EX Series switches, QFX Series switches, MX Series routers)**—The logical interface is created on ge, et, xe interfaces along with the physical interface, by default. In earlier Junos OS Releases, by default, only physical interfaces were created. For example, for ge interfaces, earlier when you view the **show interfaces** command, by default, only the physical interface (ge-0/0/0), was displayed. Now, the logical interface (ge-0/0/0.16386) is also displayed.

MPLS

- **IPv4 explicit-null label retained from the merged protocol MPLS label stack**—The IPv4 explicit-null label is retained from the merged protocol MPLS label stack, if the IPv4 explicit-null is at the bottom of the MPLS label stack.

What's Changed in Release 19.2R1

Interfaces and Chassis

- **Support to get optics loopback status for QSFP-100GE-DWDM2 transceivers (PTX Series)**—In Junos OS Release 19.2R1, and later, on PTX Series routers, you can obtain the optics loopback status of QSFP-100GE-DWDM2 transceivers along with the regular Ethernet loopback status by issuing the **show interfaces interface-name** or **show interfaces interface-name brief** command. A new output field, **Optics Loopback** is added under **Link-level type** when the **show interfaces interface-name** CLI command is executed.
- **Monitoring information available only in trace log (PTX Series)**—In Junos OS Release 19.2R1 and later, the Ethernet link fault management daemon (lfmd) in the peer router stops monitoring the locally occurred errors until unified ISSU is completed. You can view the monitoring-related details only through the trace log file.
- **Health check for power supplies (PTX10008 and PTX10016)**—Starting in Junos OS Release 19.2R1, on the PTX10008 and PTX10016 routers, the **show chassis environment pem** command displays the health check information about the DC or AC power supplies. For any power supply that does not support health check, the status is shown as **Unsupported**. The system starts health check of a power supply only if the power consumption exceeds 7 kW.

[See [show chassis environment pem](#).]

Network Management and Monitoring

- **Change in error severity (PTX10016)**—Starting in Junos OS Release 19.2R1, on PTX10016 routers, the severity of the FPC error, shown in the syslog as **PE Chip::FATAL ERROR!! from PE2[2]: RT: Clear Fatal if it is detected LLMEM Error MEM:llmem, MEMTYPE: 1**, is changed from fatal to nonfatal (or minor). In case of this error, only a message is displayed for information purposes. To view the error details, you can use the show commands **show chassis fpc errors** and **show chassis errors active**.

[See [show chassis fpc errors](#).]

- **The show system schema command and <get-yang-schema> RPC require specifying an output directory (PTX Series)**—Starting in Junos OS Release 19.2R1, when you issue the **show system schema** operational mode command in the CLI or execute the **<get-yang-schema>** RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the **<output-directory>** element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type empty (PTX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are supported only when executing the RPC in a NETCONF or Junos XML protocol session, and the value passed to the action script is the string '**none**'.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

Routing Protocols

- **Change in the default behavior of advertise-from-main-vpn-tables configuration statement**—BGP now advertises EVPN routes from the main bgp.evpn .0 table. You can no longer configure BGP to advertise the EVPN routes from the routing instance table. In earlier Junos OS Releases, BGP advertised EVPN routes from the routing instance table by default.

[See [advertise-from-main-vpn-tables](#).]

Services Applications

- **Support for enabling hardware timestamping of RPM probe messages (PTX Series)**—In Junos OS Releases 19.2R1, PTX Series routers support timestamping of RPM probe messages on the Packet Forwarding Engine. The following configuration statements at the **[edit services rpm probe owner test test-name]** hierarchy level are supported:
 - **hardware-timestamp**—To enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor.
 - **one-way-hardware-timestamp**—To enable timestamping of RPM probe messages for one-way delay and jitter measurements.

You can use these timestamping features only with icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types.

SEE ALSO

[What's New | 153](#)

[Known Limitations | 163](#)

[Open Issues | 164](#)

[Resolved Issues | 167](#)

[Documentation Updates | 170](#)

[Migration, Upgrade, and Downgrade Instructions | 171](#)

[Product Compatibility | 175](#)

Known Behavior

IN THIS SECTION

- [General Routing | 163](#)
- [Interfaces and Chassis | 164](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the PTX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- The Routing Engine boots from the secondary disk when you:

Press the reset button on the RCB front panel, while the Routing Engine is booting up but before Junos OS reboots.

Upgrade software, by booting from the network using the **request vmhost reboot network** command, and the system fails to boot from the network.

Upgrade BIOS and the upgrade fails.

Reboot and the system hangs before Junos OS reboots. [PR1344342](#)

- The command **request vmhost power-off** does not actually power off the system in the latest releases. It only does a reboot and the system comes back up. [PR1393061](#)
- Because of the small counter size present in the ASIC, the normal discard counter reported in the CLI is less than the actual packet drop rate. [PR1394979](#)

Interfaces and Chassis

- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfmd process to crash after upgrade. This is because of an old version of `/var/db/cfm.db`. [PR1281073](#)

SEE ALSO

[What's New | 153](#)

[What's Changed | 160](#)

[Open Issues | 164](#)

[Resolved Issues | 167](#)

[Documentation Updates | 170](#)

[Migration, Upgrade, and Downgrade Instructions | 171](#)

[Product Compatibility | 175](#)

Known Issues

IN THIS SECTION

- [General Routing | 165](#)
- [Infrastructure | 166](#)
- [Interfaces and Chassis | 166](#)
- [Layer 2 Ethernet Services | 166](#)
- [MPLS | 166](#)
- [Routing Protocols | 166](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for the PTX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- On a PTX Series PIC with the CFP2-DCO-T-WDM transceiver installed, after repeated configuration rollback, the link sometimes takes a long time to come up. [PR1301462](#)
- On next generation Routing-Engine (NG-RE), a failure of the Hardware Random Number Generator (HWRNG) will leave the system in a state where there is not enough entropy available to operate. [PR1349373](#)
- Unsuccessful connection attempts are not be logged on the backup SPMB. [PR1369731](#)
- Users might not be able to stop the ZTP bootstrap, when a PTX10016 or PTX10008 router with more number of line cards is powered ON with factory default configuration. [PR1369959](#)
- When a Routing Engine reboots and comes up again, it sends gratuitous ARP packets to the internal interfaces in order to advertise its MAC address. These packets get into the UKERN running on the FPC, which drops these packets. The messages are printed just before the packets are dropped. These error messages are harmless and do not disrupt the working of any feature. [PR1374372](#)
- The output of J-Flow sensor is changed for an FPC that is not configured. [PR1379770](#)
- On a PTX Series router or QFX10002, QFX10008, or QFX10016, an automatically correcting non-fatal hardware error on PE chip (which is the ASIC on PTX1000, PTX10002, and QFX10002, the third-generation FPC on PTX3000 and PTX5000, and the line card on PTX10008, PTX10016, QFX10008, and QFX10016) is reported as 'FATAL' error and hence the related Packet Forwarding Engine (PFE) gets disabled. Code changes have been made to change the error category from 'FATAL' to 'INFO' to prevent the Packet Forwarding Engine from being disabled unexpectedly. [PR1408012](#)
- When a 100g QSFP is inserted into the FPC on PTX, all the other interfaces on that FPC and the other FPCs might flap. [PR1408204](#)
- This issue is applicable to PTX Series and QFX Series devices with Express chipset. During normal operation, if the **chassis-control** process restarts, the Express ASICs are not initialized. This causes packets drop on the output queue. [PR1414434](#)
- On PTX3000 system, only if the IPLC card is present in the system, and when GRES is performed, you might observe an IPLC crash during the GRES operation. There is no impact on other line cards in the system. If there is no IPLC card in the system, there is no impact during the GRES. [PR1415145](#)
- VTY command **show filter index < number> counter** displays values as zero at 28-02-HOSTBOUND_NDP_DISCARD_TERM on PTX5000 platform. Basically the counter does not increase for NDP packets. The issue is only with **show filter index**, which is a debug tool in vty. This issue has no impact on NDP functionality for user traffic. There are no issues with NDP functionality and DDOS for NDP is also working. [PR1420057](#)
- The em2 interface configuration is causing the FPC to crash during initialization and the FPC does not come online. After deleting the em2 configuration and restarting the router FPC comes online. [PR1429212](#)

Infrastructure

- Junos OS packages might have been incorrectly registered as unsupported. [PR1427344](#)

Interfaces and Chassis

- Upgrading Junos OS Release 14.2R5 and later maintenance releases and Junos OS Release 16.1 and later mainline releases with CFM configuration might cause the cfmd process to crash after the upgrade. This is because of an old version of `/var/db/cfm.db`. [PR1281073](#)

Layer 2 Ethernet Services

- Aggregated Ethernet members take more time (greater than 5 seconds) from the physical interface up to LACP CD state when we bring laser on/off on 25% of the 10-Gigabit aggregated Ethernet members. [PR1415615](#)

MPLS

- The optimization timer is being updated in an incorrect manner in the code path. Due to this, a particular check fails when the exponential increase function is called. This code path is now fixed. [PR1416948](#)

Routing Protocols

- When the loopback interface is configured in a logical-system and Routing Engine-based micro BFD is configured to use the loopback address as the source address, BFD packets go out with the source address belonging to the outgoing interface rather than the loopback address. Due to this issue, the micro BFD session might not be able to come up. [PR1370463](#)
- The PTX Series device cannot intercept the PIM BSR message and thus cannot participate in DF election when BSR is used. [PR1419124](#)

SEE ALSO

[What's New | 153](#)

[What's Changed | 160](#)

[Known Limitations | 163](#)

[Resolved Issues | 167](#)

[Documentation Updates | 170](#)

Migration, Upgrade, and Downgrade Instructions | 171

Product Compatibility | 175

Resolved Issues

IN THIS SECTION

- General Routing | 167
- Infrastructure | 169
- Interfaces and Chassis | 169
- MPLS | 169
- Platform and Infrastructure | 169
- Routing Protocols | 169

This section lists the issues fixed in Junos OS Release 19.2R1 for the PTX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- Repeated log messages **%PFE-3 fpcX expr_nh_index_tree_ifl_get and expr_nh_index_tree_ipaddr_get** are observed when a sampling packet is discarded with the log (or syslog) statement under the firewall filter. [PR1304022](#)
- Disable reporting of the correctable single-bit error on Hybrid Memory Cube (HMC) and prevent a major alarm. [PR1384435](#)
- CPU overuse might be observed on PTX/QFX10000 Series platform. [PR1399369](#)
- The DHCPv6 relay-reply packet might be dropped by the DHCP relay. [PR1399683](#)
- Only one Packet Forwarding Engine could be disabled on an FPC with multiple Packet Forwarding Engines in an error/wedge condition. [PR1400716](#)
- The TCP connection between pppmd and pppman might be dropped because of a kernel issue. [PR1401507](#)
- Log message **JAM HW data base open failed for ptx5kpic_3x400ge-cfp8** during commit. [PR1403071](#)
- The **Incorrect mem stats** message is seen in the logs of PTX Series Type 1 FPC. [PR1404088](#)

- On a PTX3000, FPCs are not able to come online for tens of minutes after a reboot of the chassis. [PR1404611](#)
- ZTP upgrade failed. Image file transfer got stalled during the ZTP process. [PR1404832](#)
- On PTX3000 and PTX5000, the backup CB's chassis environment status is displayed as Testing after the backup CB is removed and reinserted. [PR1405181](#)
- The 100-gigabit SR4 optics with part number 740-061405 should be displayed as **QSFP-100G-SR4-T2**. [PR1405399](#)
- Layer 2 VPN might flap repeatedly after the link up between the PE device and CE device comes up. [PR1407345](#)
- Ports 4, 5, 14, 15, 24, and 25 on PTX10K-LC1101/PTX10K-LC1105 might fail to come up after the device is upgraded to Junos OS Release 17.4R2-S3. [PR1407655](#)
- **openconfig-network-instance:network-instances** support for IS-IS must be hidden unless supported. [PR1408151](#)
- [PTX3000-CI] : Observing rpd crash @
`if_addr_link,krt_chnh_template_create_restart,krt_chnh_create_restart,krt_comp_add_comp_nh,
krt_build_comp_nh,krt_build_nexthop,krt_rt_add_sock,krt_decode_rt,krt_sysctl_read_consume,
krt_rt_read,krt_sys_rtread,krt_var_init,ctx_handle_node,ctx_walk_features,task_read_config,main`
[PR1409051](#)
- PTX Series Inline J-Flow : FPC goes offline when the sampling rate is changed at runtime to 80000;also dcpfe core file was generated. [PR1409502](#)
- The port on the FPC (for example, JNP10K-LC1101) might fail to come up. [PR1409585](#)
- Hostname does not update at FPC shell after system configuration change on CLI. [PR1412318](#)
- Junos OS PCC might reject PCUpdate/PCCreate message if the metric type is other than type 2. [PR1412659](#)
- The L2 circuit egress PE might drop the traffic in a FAT+CW enabled L2 circuit scenario when another FAT+CW enabled L2 circuit PW flaps. [PR1415614](#)
- Traffic loss could be seen for the duration of the hold-time down timer when flapping an interface with hold-time down timer configured. [PR1418425](#)
- Error messages might be seen on PTX10000/QFX10000 platforms during DFE tuning. [PR1421075](#)
- Virtual Chassis might become unstable and FXPC core files might be generated when there are a lot of configured filter entries. [PR1422132](#)
- While committing a huge configuration, the customer sees the error **error: mustd trace init failed**.[PR1423229](#)
- Traffic is dropped after an FPC reboot with aggregated Ethernet member links deactivated by the remote device. [PR1423707](#)

- A specific interface on the P3-15-U-QSFP28 PIC remains down until another interface comes up. [PR1427733](#)
- The output of **show chassis environment** shows Input0 and Input1. [PR1428690](#)

Infrastructure

- The **request system recover oam-volume** command might fail on PTX Series routers. [PR1425003](#)

Interfaces and Chassis

- Syslog message **/kernel: %KERN-3: pointchange for flag 04000000 not supported on IFD aex** upon LFM related configuration commit on ae interfaces. [PR1423586](#)
- Some ports on PTX Series routers might remain down after the FPC or device at the remote side is rebooted. [PR1429315](#)

MPLS

- An RSVP-signaled LSP might stay in the down state after a link in the path flaps. [PR1384929](#)
- LDP route flap during unrelated commit. [PR1416032](#)
- Bypass dynamic RSVP LSP tears down too soon when being used for protecting the LDP LSP with the **dynamic-rsvp-lsp** statement. [PR1425824](#)

Platform and Infrastructure

- RPM hardware-timestamp and **one-way-hardware-timestamp** statements are not enabled. [PR1399842](#)

Routing Protocols

- A syslog message is seen whenever the prefix SID coincides with the node sid. [PR1403729](#)
- An rpd memory leak might be seen in an IS-IS segment routing scenario. [PR1404134](#)
- Dynamic routing protocol flapping with vmhost Routing Engine switchover on NG-RE. [PR1415077](#)
- Route churn occurs when a nonrelevant configuration is changed. [PR1423647](#)
- RPD might crash with **ospf overload as-external** configuration. [PR1429765](#)

SEE ALSO

What's New	 153
What's Changed	 160
Known Limitations	 163
Open Issues	 164
Documentation Updates	 170
Migration, Upgrade, and Downgrade Instructions	 171
Product Compatibility	 175

Documentation Updates

IN THIS SECTION

- [Installation and Upgrade Guide](#) | [170](#)

This section lists the errata and changes in Junos OS Release 19.2R1 documentation for the PTX Series.

Installation and Upgrade Guide

- **Veriexec explained (PTX Series)**—Verified Exec (also known as veriexec) is a file-signing and verification scheme that protects the Junos operating system (OS) against unauthorized software and activity that might compromise the integrity of your device. Originally developed for the NetBSD OS, veriexec was adapted for Junos OS and enabled by default from Junos OS Release 7.5 onward.

[See [Veriexec Overview](#).]

SEE ALSO

What's New	 153
What's Changed	 160
Known Limitations	 163
Open Issues	 164
Resolved Issues	 167
Migration, Upgrade, and Downgrade Instructions	 171

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 19.2 | 171](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 174](#)
- [Upgrading a Router with Redundant Routing Engines | 174](#)

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the PTX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading to Release 19.2

When upgrading or downgrading Junos OS, use the **jinstall** package. For information about the contents of the **jinstall** package and details of the installation process, see the [Installation and Upgrade Guide](#). Use other packages, such as the **jbundle** package, only when so instructed by a Juniper Networks support representative.

NOTE: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

```
user@host> request system snapshot
```

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the router, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and SSH files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the [Installation and Upgrade Guide](#).

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

To download and install Junos OS Release 19.2R1:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:
<https://support.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Click the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the router.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

All customers except the customers in the Eurasian Customs Union (currently comprised of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

```
user@host> request system software add validate reboot
source/junos-install-ptx-x86-64-19.2R1.9.tgz
```

Customers in the Eurasian Customs Union (currently comprised of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos OS package):

```
user@host> request system software add validate reboot
source/junos-install-ptx-x86-64-19.2R1.9-limited.tgz
```

Replace the **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
 - **ftp://hostname/pathname**
 - **http://hostname/pathname**
 - **scp://hostname/pathname**

The **validate** option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Adding the **reboot** command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).

NOTE: After you install a Junos OS Release 19.2jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

NOTE: Most of the existing **request system** commands are not supported on routers with RE-PTX-X8 Routing Engines. See the VM Host Software Administrative Commands in the [Installation and Upgrade Guide](#).

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://support.juniper.net/support/eol/software/junos/>.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the [Installation and Upgrade Guide](#).

SEE ALSO

[What's New | 153](#)

[What's Changed | 160](#)

[Known Limitations | 163](#)

[Open Issues | 164](#)

[Resolved Issues | 167](#)

[Documentation Updates | 170](#)

[Product Compatibility | 175](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 175](#)

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on PTX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

What's New	 153
What's Changed	 160
Known Limitations	 163
Open Issues	 164
Resolved Issues	 167
Documentation Updates	 170
Migration, Upgrade, and Downgrade Instructions	 171

Junos OS Release Notes for the QFX Series

IN THIS SECTION

- [New and Changed Features](#) | [177](#)
- [Changes in Behavior and Syntax](#) | [186](#)
- [Known Behavior](#) | [188](#)
- [Known Issues](#) | [190](#)
- [Resolved Issues](#) | [197](#)
- [Documentation Updates](#) | [204](#)
- [Migration, Upgrade, and Downgrade Instructions](#) | [205](#)
- [Product Compatibility](#) | [219](#)

These release notes accompany Junos OS Release 19.2R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [New and Changed Features: 19.2R1-S1 | 177](#)
- [New and Changed Features: 19.2R1 | 178](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for the QFX Series.

NOTE: The following QFX Series platforms are supported in Release 19.2R1: QFX5100, QFX5110 (32Q and 48S), QFX5120, QFX5200, QFX5200-32CD, QFX5210, QFX10002, QFX10002-60C, QFX10008, and QFX10016.

Junos on White Box runs on Accton Edgecore AS7816-64X switches in this release. The software is based on Junos OS running on QFX5210 switches, so release-note items that apply to QFX5210 switches also apply to Junos on White Box.

New and Changed Features: 19.2R1-S1

EVPN

- **Overlay load balancing in an EVPN-VXLAN network (QFX5200 and QFX5210 switches)**—Starting in Junos OS Release 19.2R1-S1, QFX5200 and QFX5210 switches that function as leaf or spine devices in an EVPN-VXLAN network (centrally-routed and edge-routed bridging overlays) support load balancing among different virtual tunnel endpoints (VTEPs). We support overlay load balancing in the following use cases:
 - A leaf device is multihomed to multiple spine devices.
 - A host is multihomed to multiple leaf devices.

In both use cases, each multihomed physical, aggregated Ethernet, or logical interface is configured with an Ethernet segment identifier (ESI). Overlay load balancing supports a maximum of 255 ESIs. If you exceed this maximum (for example, you configure 256 ESIs), traffic destined for the 256th ESI is flooded to the VLAN associated with the ESI.

To enable overlay load balancing, enter the **vxlan-overlay-load-balance** configuration statement at the **[edit forwarding-options]** hierarchy level.

[See the [EVPN User Guide](#).]

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Hardware

- **5.5 KW Power Supplies (QFX10000 switches)**—Starting in Junos OS Release 19.2R1, QFX10000 modular chassis adds two 5.5 KW power supplies. The JNP10K-PWR-AC2 power supply supports AC, high-voltage alternating current (HVAC), DC, or high-voltage direct current (HVDC). The JNP10K-PWR-DC2 provides a 5.5 KW upgrade for DC users. Two new ordering SKUs are available for the QFX10008 switch: QFX10008-BASE-H and QFX10008-REDUND-H.

The JNP10K-PWR-AC2 takes AC input and provides DC output of 12.3 VDC, 5000 W with a single feed and 5500 W with a dual feed. For AC systems, the operating input voltage is 180 to 305 VAC and for DC systems, the operating input voltage is 190 to 410 VDC.

The JNP10K-PWR-DC2 power supply provides two power supplies in a single housing that accepts either 60 A or 80 A using four redundant input power feeds. PS_0 and PS_1 each have redundant input feeds: A0 and/or B0 for PS_0 and A1 and/or B1 for PS_1. The input is configured using a set of dip switches on the power supply faceplate. The output is dependent on the settings of these dip switches.

[See [QFX10008 System Overview](#).]

EVPN

- **EVPN-VXLAN support (QFX10002-60C switches)**—Starting in Junos OS Release 19.2R1, the QFX10002-60C switch can function as a Layer 2 or Layer 3 VXLAN gateway in both EVPN-VXLAN centrally-routed and edge-routed bridging overlays (EVPN-VXLAN topologies with two-layer and collapsed IP fabrics). In these roles, the switch supports the following features:
 - Enterprise style of Layer 2 interface configuration
 - Active/active multihoming
 - Default routing instance
 - Multiple routing instances of type virtual switch, and VLAN-aware service on the virtual switch routing instance
 - Pure type-5 routes
 - Proxy ARP use and ARP suppression, and proxy NDP use and NDP suppression on an IRB interface
 - ESIs on physical and aggregated Ethernet interfaces

- OSPF, IS-IS, BGP, and static routing on IRB interfaces
- DHCP relay
- IPv6 support for user data traffic
- EVPN-VXLAN with MPLS as transport layer
- MAC mobility

[See [EVPN User Guide](#).]

- **Unicast VXLAN with MC-LAG (QFX5120 switches)**—Instead of EVPN providing remote VXLAN tunnel endpoint (remote VTEP) reachability information, starting in Junos OS Release 19.2R1, Junos OS supports the static configuration of remote VTEPs on QFX5120 switches in a network that also includes the following elements:
 - Endpoints multihomed to a pair of QFX5120 switches, each of which functions as Layer 2 VXLAN gateways or leaf devices, and as MC-LAG peers
 - Spine devices functioning as Layer 3 devices that handle the QFX5120 switches' IPv4 traffic

In this environment, the QFX5120 switches also support the configuration of ingress node replication, which enables the replication of Layer 2 BUM traffic. In fact, when you configure ingress node replication, other multicast features are disabled.

Interfaces and Chassis

- **Domain Name System (DNS) is VRF aware (QFX Series)**—Starting in Junos OS Release 19.2R1, when the **management-instance** statement is configured at the **[edit system]** hierarchy level, you can use the non-default management routing instance `mgmt_junos` as the routing instance through which the DNS name server is reachable. To specify the routing instance `mgmt_junos`, configure our new configuration statement **routing-instance mgmt_junos**, at the **[edit system name-server server-ip]** hierarchy level.

[See [Management Interface in a Nondefault Instance, Configuring a DNS Name Server for Resolving a Hostname into Addresses](#), [name-server](#), and [show host](#).]

- **Uplink failure detection debounce interval (QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210 switches)**—Starting with Junos OS Release 19.2R1, you can configure the debounce interval, which is an amount of time, in seconds, that elapses before the downlink interfaces are brought up after corresponding state change of the uplink interfaces. In the absence of a debounce interval configuration, the downlink interfaces are brought up immediately after a state change of the uplink interfaces, which might introduce unnecessary state changes of the downlink interfaces, as well as unnecessary failovers on the servers connected to these ports.

You can configure the **debounce-interval** statement at the **[edit protocols uplink-failure-detection group group-name]** hierarchy level.

[See [Uplink Failure Detection](#).]

Junos OS XML, API, and Scripting

- **Automation script library additions and upgrades (QFX Series)**—Starting in Junos OS Release 19.2R1, devices running Junos OS that support the Python extensions package include new and upgraded Python modules. Python automation scripts can leverage new on-box Python modules, including the **requests**, **chardet**, and **urllib3** modules, as well as upgraded versions of the **idna**, **ipaddress**, and **six** modules. The Requests library provides additional methods for supporting initial deployments as well as for performing routine monitoring and configuration changes on devices running Junos OS.

[See [Overview of Python Modules Available on Devices Running Junos OS](#) and [Using the Requests Library for Python on Devices Running Junos OS](#).]

Junos Telemetry Interface

- **Sensor level statistics support on Junos Telemetry Interface (JTI) (MX960, MX2008, MX2010, MX2020, PTX5000, PTX1000, and PTX10000 routers and QFX5100 and QFX5200 switches)**—Starting with Junos OS Release 19.2R1, you can issue the Junos operational mode command **show network-agent statistics** to provide more information on a per-sensor level for statistics being streamed to an outside collector by means of remote procedure calls (gRPC) and JTI. Only sensors exported with gRPC are supported. The command does not support UDP-based sensors.

[See [show network-agent statistics](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **ONCE mode supported using gNMI services and JTI (QFX Series)**—Starting in Junos OS Release 19.2R1, you can include the "ONCE" mode with the **Subscribe** RPC when subscribing to gRPC Network Management Interface (gNMI) services to export statistics for telemetry monitoring and management using Junos telemetry interface (JTI). ONCE mode ensures that the collector is only streamed telemetry information one time at initial connection establishment? .

The subscribe RPC and subscription parameters are defined in the [gnmi.proto](#) file.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support JTI.

[See [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **Packet Forwarding Engine statistics export using gNMI and JTI (QFX5100 and QFX5200 switches)**—Starting in Junos OS Release 19.2R1, you can stream Packet Forwarding Engine statistics to an outside collector using gRPC Management Interface (gNMI) version 0.7.0 and Junos telemetry interface (JTI). Prior to this, these statistics were exported using OpenConfig gRPC and UDP protocol buffer (gpb) format. OpenConfig gRPC and gNMI are both protocols used to modify and retrieve configurations as well as export telemetry streams from a device in order to manage and monitor it

To provision Packet Forwarding Engine sensors to export data through gNMI, use the subscribe RPC defined in the [gnmi.proto](#) to specify request parameters. This RPC already supports Routing Engine statistics to be exported by means of gNMI. Now, Packet Forwarding Engine sensors will also stream KV pairs in gNMI format for a majority of Packet Forwarding Engine sensors.

Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#) and [Understanding OpenConfig and gRPC on Junos Telemetry Interface](#).]

- **gNMI support extended for JTI (QFX5110, QFX5120, QFX5200, and QFX5210 switches)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) sensor support extends the ability to configure the following resource paths that use gRPC for export to also use gRPC Management Interface (gNMI) for export. gNMI is a protocol for configuration and retrieval of state information.

JTI supports the following resource paths:

- `/components/component/properties/property/state/value`
- `/components/component/state/`
- `/interfaces/interface/state/`
- `/interfaces/interface/subinterfaces/subinterface/state/`

To provision the sensor to export data through gNMI, use the Subscribe RPC defined in the [gnmi.proto](#) to specify request parameters. Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **gNMI support for Routing Engine statistics for JTI (QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210 switches)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) supports the export of Routing Engine sensors using gRPC Management Interface (gNMI). gNMI is a protocol for configuration and retrieval of state information.

You can use gNMI to export the following statistics:

- LACP state export (resource path `/lacp/interfaces/interface[name='ae1']/members/member/`)
- LLDP statistics (resource path `/lldp/interfaces/interface[name='xe-0/0/9']/`)
- BGP peer information (for example, resource path `/network-instances/network-instance/protocols/protocol/bgp/neighbors/neighbor/`)
- RSVP interface statistics (resource path `/junos/rsvp-interface-information/`)
- RPD task memory utilization (resource path `/junos/task-memory-information/`)
- LSP event export (resource path `/junos/task-memory-information/`)

To provision the sensor to export data through gNMI, use the `telemetrySubscribe` RPC to specify telemetry parameters. Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the Junos Telemetry Interface (JTI).

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **gNMI support for Packet Forwarding Engine sensors for JTI (QFX5200 switches)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) supports the export of Packet Forwarding Engine sensors using gRPC Management Interface (gNMI). gNMI is a protocol for configuration and retrieval of state information.

You can stream the following statistics using gNMI for export:

- Congestion and latency monitoring (resource path `/junos/system/linecard/qmon-sw/`)
- Logical interface usage (resource path `/junos/system/linecard/interface/logical/usage`)
- Filter statistics (resource path `/junos/system/linecard/firewall/`)
- Physical interface statistics (resource path `/junos/system/linecard/interface`)
- LSP statistics (resource path `/junos/services/label-switched-path/usage/`)
- NPU and line-card statistics (resource path `/junos/system/linecard/cpu/memory/`)

To provision the sensor to export data through gNMI, use the Subscribe RPC defined in the [gnmi.proto](#) to specify request parameters. Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **gNMI support for Routing Engine statistics for JTI (QFX5200 switches)**—Starting in Junos OS Release 19.2R1, Junos telemetry interface (JTI) supports export of Routing Engine sensors using gRPC Management Interface (gNMI). gNMI is a protocol for configuration and retrieval of state information. Both streaming and ON_CHANGE export is supported using gNMI.

Export the following statistics using gNMI:

- Network discovery, ARP table state (resource path `/arp-information/`)
- Network discovery, NDP table state (resource paths `/nd6-information/` and `/ipv6-ra/`)

To provision the sensor to export data through gNMI, use the Subscribe RPC defined in the [gnmi.proto](#) to specify request parameters. Streaming telemetry data through gNMI also requires the OpenConfig for Junos OS module. Starting in Junos OS Release 18.3R1, OpenConfig and Network Agent packages are bundled into the Junos OS image by default. Both packages support the JTI.

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

- **Specify Routing Instance for JTI (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 19.2R1, you can specify the routing instance to use for remote procedure call (gRPC) services. Include the **routing-instance** *instance-name* at the `[edit system services extension-service request-response grpc]` hierarchy level. The routing instance name specified should match the name of the existing routing instance, such as a name configured under the `[routing-instances]` hierarchy level

or `mgmt_junos` if `system management-instance` is configured (the dedicated management routing instance).

Configuring the routing instance lets you choose the VRF for gRPC services. When the routing instance is not configured, the default behavior is that all gRPC-related services are available through the management `fxp0/em0` interface.

MPLS

- **Support for MPLS firewall filter on loopback interface (QFX5100, QFX5110, QFX5200, QFX5210)**—Starting with Junos OS Release 19.2R1, you can apply an MPLS firewall filter to a loopback interface on a label-switching router (LSR). For example, you can configure an MPLS packet with `ttl=1` along with MPLS qualifiers, such as `label`, `exp`, and Layer 4 `tcp/udp` port numbers. Supported actions include `accept`, `discard`, and `count`. You configure this feature at the `[edit firewall family mpls]` hierarchy level. You can only apply a loopback filters on `family mpls` in the ingress direction.

[See [Overview of MPLS Firewall Filters on Loopback Interface](#).]

- **Support for IS-IS segment routing (QFX10002-60C)**—Starting in Junos OS Release 19.2R1, you can use IS-IS segment routing through MPLS. Currently, label advertisements are supported for IS-IS only. IS-IS creates an adjacency segment per adjacency, per level, and per address family (one each for IPv4 and IPv6). Junos OS IS-IS implementation allocates node segment label blocks in accordance with the IS-IS protocol extensions for supporting segment routing node segments. It provides a mechanism to the network operator to provision an IPv4 or IPv6 address family node segment index. To configure segment routing, use the following configuration statements at the `[edit protocols isis]` hierarchy level:
 - **source-packet-routing**—Enable the source packet routing feature.
 - **node-segment**—Enable source packet routing at all levels.
 - **use-source-packet-routing**—Enable use of source packet routing node segment labels for computing backup paths for normal IPv4 or IPv6 IS-IS prefixes and for primary IS-IS source packet routing node segments.
 - **no-advertise-adjacency-segment**—Disable advertising of the adjacency segment on all levels for a specific interface.

[See [Understanding Source Packet Routing in Networking \(SPRING\)](#).]

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (QFX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data model when you include the `action-expand` extension statement in the option or statement definition and reference a script that handles the logic. The `action-expand` statement must include the `script` child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules.](#)]

- **Remote port mirroring and remote port mirroring to an IP address (QFX10002-60C switch)**—Starting with Junos OS Release 19.2R1, use port mirroring to copy packets entering or exiting a port or entering a VLAN and send the copies to a VLAN for remote monitoring. You can also send mirrored packets to an IP address over a Layer 3 network (for example, if there is no Layer 2 connectivity to the analyzer device). Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.

[See [Understanding Port Mirroring.](#)]

Routing Policy and Firewall Filters

- **Support for interface, forwarding-class, and loss priority match conditions on egress interfaces (QFX10002-36Q, QFX10002-72Q, QFX10002-60C, QFX10008, QFX10016)**—Starting with Junos OS Release 19.2R1, you can apply the **interface**, **forwarding-class**, and **loss-priority** firewall filter match conditions in the egress direction on IPv4 and IPv6 interfaces. You configure the match conditions at the **[edit firewall]** hierarchy level. This feature was previously supported in an "X" release of Junos OS.

[See [Firewall Filter Match Conditions and Actions \(QFX10000\).](#)]

- **Loopback firewall filter scale optimization (QFX5120)**—Starting with Junos OS Release 19.2R1, you can increase the number of ingress firewall filters on the loopback interface from 384 to 768. To do this, you configure an ingress firewall filter, apply it to the loopback interface, and then use the **loopback-firewall-optimization** command at the **[edit chassis] hierarchy level** to enable optimization. When you configure the loopback filter, you must explicitly specify the terms for **reserved multicast destination** and **ttl** exception packets for this feature to work properly. Enabling or disabling optimization causes the PFE process to restart. This flaps the interfaces, meaning they go up and down, so traffic drops are expected.

[See [Planning the Number of Firewall Filters to Create.](#)]

Routing Protocols

- **Support for 512 ECMP next hops for BGP (QFX10000 switches)**—Starting with Junos OS Release 19.2R1, you can configure a maximum of 512 equal-cost multipath (ECMP) next hops for external BGP peers. (Previously, the maximum number supported was 128.) Having the ability to configure up to 512 ECMP next hops allows you to increase the number of direct BGP peer connections with the QFX10000 switches, thus improving latency and optimizing data flow. Optionally, you can configure those ECMP paths to use consistent load balancing (consistent hashing).

NOTE: This feature applies only to routes for external BGP peers. It does not apply to MPLS routes.

[See [Understanding Configuration of Up to 512 Equal-Cost Paths With Optional Consistent Load Balancing.](#)]

- **Support for export of BGP Local RIB through BGP Monitoring Protocol (BMP) (QFX Series)**—Starting in Junos OS Release 19.2R1, BMP is enhanced to support monitoring of local RIB (**loc-rib**) policy. The **loc-rib** policy is added to RIB types under the **bmp route-monitoring** statement.

[See: [Understanding the BGP Monitoring Protocol.](#)]

Software Installation and Upgrade

- **The curl binary is packaged and made available on all Junos OS variants (QFX Series)**—The curl binary is a command-line utility, used from the shell, that you can use to perform operations over several transport protocols, including the following: dict, file, ftp, gopher, http, imap, pop3, rtsp, smtp, telnet, tftp. The features enabled on Junos OS are curl version 7.59, libcurl version 7.59.
- **In-service software upgrade (ISSU) and in-service software reboot (ISSR) (QFX5200 switches)**—Starting with Junos OS Release 19.2R1, you can perform an in-service software upgrade (ISSU) to upgrade between two different Junos OS releases with minimal data and control-plane traffic impact. You can also perform an in-service software reboot (ISSR), which enables you to reset the software state of the system with minimal disruption in data and control traffic.

You can perform an ISSU by issuing the **request system software in-service-upgrade package-name** command.

You can perform an ISSR by issuing the **request system reboot in-service** command.

[See [Understanding In-Service Software Upgrade \(ISSU\).](#)]

System Management

- **Support for transferring accounting statistics files and router configuration archives using HTTP URL (QFX Series)**—Starting in Junos OS Release 19.2R1, you can transfer accounting statistics files and router configuration archives to remote servers by using an HTTP URL. In addition to SCP and FTP, the following HTTP URL will be supported under the **archive-sites** statement:

http://username@host:url-path password password

- To transfer accounting statistics files, configure **archive-sites** under **[edit accounting-options file <filename>]** hierarchy.
- To transfer router configuration archival, configure **archive-sites** under **edit system archival configuration** hierarchy.
- To view the statistics of transfer attempted, succeeded, and failed, use the **show accounting server statistics archival-transfer** command.
- To clear the statistics of transfer attempted, succeeded, and failed, use the **clear accounting server statistics archival-transfer** command.

[See [archive-sites](#), [Backing Up Configurations to an Archive Site](#), [show accounting server statistics archival-transfer](#), and [clear accounting server statistics archival-transfer](#)].

SEE ALSO

[What's Changed | 186](#)

[Known Limitations | 188](#)

[Open Issues | 190](#)

[Resolved Issues | 197](#)

[Documentation Updates | 204](#)

[Migration, Upgrade, and Downgrade Instructions | 205](#)

[Product Compatibility | 219](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Interfaces and Chassis | 186](#)
- [Network Management and Monitoring | 187](#)
- [Security | 187](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the QFX Series.

Interfaces and Chassis

- **The resilient-hash statement is no longer available under aggregated-ether-options (QFX5200 and QFX5210 switches)**—Starting in Junos OS Release 19.2R1, the **resilient-hash** statement is no longer available at the **[edit interfaces aex aggregated-ether-options]** hierarchy level. Resilient hashing is not supported on LAGs on QFX5200 and QFX5210.

[See [aggregated-ether-options](#).]

- **Logical interfaces created along with physical interfaces by default (QFX10000 and QFX5000 switches)**—On the QFX10000 line of switches, logical interfaces are created along with the physical et-, sxe-, xe-, and channelized xe- interfaces. In earlier releases, only physical interfaces are created.

On the QFX5000 line of switches, by default, logical interfaces are created on channelized xe- interfaces. In earlier releases, logical interfaces are not created by default on channelized xe- interfaces (xe-0/0/0:1, xe-0/0/0:2, and so on), but they are created on et-, sxe-, and nonchannelized xe- interfaces.

- **Health check for power supplies (QFX10008)**—Starting in Junos OS Release 19.2R1, on the QFX10008 switches, the **show chassis environment pem** command displays the health check information about the DC or AC Power supplies. For any power supply that does not support health check, the status is shown as **Unsupported**. The system starts health check of a power supply only if the power consumption exceeds 7 KW.

[See [show chassis environment pem](#)]

Network Management and Monitoring

- **The show system schema command and <get-yang-schema> RPC require specifying an output directory (QFX Series)**—Starting in Junos OS Release 19.2R1, when you issue the **show system schema** operational mode command in the CLI or execute the **<get-yang-schema>** RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the **<output-directory>** element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type empty (QFX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are supported only when you execute the RPC in a NETCONF or Junos OS XML protocol session, and the value passed to the action script is the string '**none**'.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

Security

- **Firewall warning message (QFX5000 switches)**—Starting in 19.2R1, a warning message is displayed whenever a firewall term includes **log** or **syslog** with the **accept** filter action.

SEE ALSO

[What's New | 177](#)

[Known Limitations | 188](#)

Open Issues 190
Resolved Issues 197
Documentation Updates 204
Migration, Upgrade, and Downgrade Instructions 205
Product Compatibility 219

Known Behavior

IN THIS SECTION

- [EVPN | 188](#)
- [General Routing | 188](#)
- [Layer 2 Features | 189](#)
- [Routing Protocols | 189](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the QFX Series.

For the most complete and latest information about known Junos OS problems, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- When a VLAN uses an IRB interface as the routing interface, the vlan-id parameter must be set to none to ensure proper traffic routing. [PR1287557](#)

General Routing

- When the sFlow collector can be reached only through the Routing Engine, large samples because the heavy traffic might cause the Routing Engine CPU to become busy. [PR1332337](#)
- On the QFX5100, if a scaled configuration involving a LAG interface, more than 3000 VLANs, and the corresponding next hops is removed and a new configuration involving a LAG interface is applied at the same time, the new configuration might not take effect until the previous configuration has been deleted. During this time, the fxpc process might consume high CPU resources. No other system impact is observed. [PR1363896](#)

- Error logs are expected when routes point to the target next hop, which in turn point to hold next hops. These error logs are present for a short time. Later, when the next hop changes from a hold next hop to valid next hop, unlist next hops will be walked again and updated with the appropriate weight and reroute counters, and no more error logs will be seen. [PR1387559](#)
- In case the out-of-band management link is operated at a speed other than 1000 Mbps (for example, link peer is kept 10 or 100 Mbps) on QFX Series devices (where supported) - within the Junos VM, the corresponding interface always reflects a speed of 1000 Mbps in all aspects—for example, in the output of the **show interfaces** command (example, **show interfaces em0**). The actual speed in use is displayed only on the corresponding interface on the Linux host. [PR1401382](#)
- USB install: If the USB storage device is not removed from your device after a USB upgrade, the system does not come up and keeps rebooting. You must manually change the boot sequence from BIOS menu to select boot from SSD. PXE install: The system boots twice from PXE before booting from SSD. This increases boot time. [PR1404717](#)
- Maximum egress L3 interfaces that can be configured on QFX5100 is 8000, QFX5200 is 8000, and QFX5110 is 12,000. [PR1406107](#)
- For a GRE physical interface and logical interface, the packets per second (pps) and bytes per second (bps) statistics always show zero. [PR1419321](#)
- When the GRE tunnel destination is reachable through an ECMP path and the ECMP's child next-hop gets modified, the GRE logical interface statistics might reset. However, the GRE physical interface will reflect the correct statistics. [PR1421069](#)
- Downgrade from Junos OS Release 19.2 to Junos OS Release 17.2X75-D42 can be done by USB install only. [PR1427984](#)

Layer 2 Features

- The **targeted-broadcast forward-only** command does not broadcast the traffic. [PR1359031](#)

Routing Protocols

- When an interface is configured with family **mpls**, one label is reserved for explicit-null case. Only one label will be used across the different MPLS interfaces for explicit-null case. This label might only be deleted when all the interfaces with family **mpls** are deleted. So the maximum number of tunnels that you can have is 1. [PR1418733](#)
- When IRACL v6 and loopback v6 entries are present, deletion and rollback of loopback v6 configuration might take time to re-program the entries in hardware. This is because loopback v6 has a high priority in the same IRACL groups and the existing IRACL v6 entries have to be re-shuffled in the hardware. [PR1428087](#)

SEE ALSO

What's New		177
What's Changed		186
Open Issues		190
Resolved Issues		197
Documentation Updates		204
Migration, Upgrade, and Downgrade Instructions		205
Product Compatibility		219

Known Issues

IN THIS SECTION

- [EVPN](#) | [190](#)
- [General Routing](#) | [191](#)
- [Layer 2 Ethernet Services](#) | [194](#)
- [Layer 2 Features](#) | [194](#)
- [MPLS](#) | [196](#)
- [Platform and Infrastructure](#) | [196](#)
- [Routing Protocols](#) | [196](#)

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for the QFX Series switches.

For the most complete and latest information about known Junos OS problems, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- At times, when I2ald is restarted, a race condition occurs where VTEP notification comes in from the kernel before Io0. As a result, I2ald is unable to process the VTEP add request and gets stuck in an indefinite loop. [PR1384022](#)
- The **show evpn instance extensive esi** command does not filter output by ESI. [PR1402175](#)

General Routing

- L3 multicast traffic does not converge to 100 percent and continuous drops are observed after the downstream interface goes down or comes up or while an FPC comes online after restarting. This happens with multicast replication for 1000 VLAN/IRB interfaces. [PR1161485](#)
- Port LEDs on the QFX5100 do not work. If a device connects to a port on the QFX5100, the port LED stays unlit. [PR1317750](#)
- The BFD session over an aggregated Ethernet interface flaps when a member link carrying the BFD Tx flaps. [PR1333307](#)
- QFX10000 platform drops the Aruba wireless access point (AP) heartbeat packets. As a result, the Aruba wireless AP cannot work. [PR1352805](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- The time lapse between interface-down interrupt detection to FRR callback is approximately 148 ms on the QFX5120 platform, although the in-place update FRR programming is completed in 1 ms. The minimum FRR time achieved with this limitation is 150 ms and the maximum is 275 ms approximately. [PR1364244](#)
- From Junos OS Release 17.3R1, on a QFX10002 platform, in a rare condition, the IPFIX flow statistics (packet/byte counters) are incorrect in the exported record. Because the statistics are not collected properly, the flow might time out and get deleted because of an inactive timeout, causing exported records to be sent out unexpectedly. Traffic spikes generated by IPFIX might be seen. [PR1365864](#)
- The `pm4x25_line_side_phymod_interfa` statement might throw the error **ERROR: u=0 p=81 interface type 16 not supported by internal SERDES for this speed 50000**. This error message is seen when channelization is detected in the Junos OS Release 18.1R3. [PR1366137](#)
- User might not be able to stop the ZTP bootstrap, when a QFX10016/QFX10008 router with more number of line cards is powered on with factory default configuration. [PR1369959](#)
- `request virtual-chassis vc-port diagnostics optics` followed by `show virtual-chassis vc-port diagnostics optics` might not show information from Virtual Chassis members apart from the master. [PR1372114](#)
- The static speed 100 MB remains the same after you change the 100M setting to autonegotiation. [PR1372647](#)
- Auto-configured VCP links might not come up if the existing member that is connected through the auto-configured VCP is removed and added back. [PR1375913](#)
- When the `show` command is taking a long time to display results, the STP might change states as BPDUs are no longer processed and cause lots of outages. [PR1390330](#)
- The `dcpe` process did not come up in some instances when the QFX5120 was abruptly powered off and powered on, and power cycling of the device or host reboot will recover the device. [PR1393554](#)

- If PTP transparent clock is configured on the QFX5200, and if **IGMP snooping** is configured for the same VLAN as PTP traffic, the PTP over Ethernet traffic might be dropped. [PR1395186](#)
- On QFX5110, multiple FANs multiple FAN LEDs might be lit solid amber although there is no hardware failure. [PR1398349](#)
- L2 multicast and broadcast convergence is high while deleting and adding back the scale configurations of VLANs and VXLANs. [PR1399002](#)
- On QFX5100, traffic initiated from a server connected to an interface is dropped at the interface on the switch if the interface is configured with family **ethernet-switching** with VXLAN and the configuration is changed to family **inet**. [PR1399733](#)
- On a QFX5120 system transition from VXLAN/EVPN collapsed to non-collapsed L2 or L3 gateway and vice versa need switch reload because of stale source VTEP IP. [PR1405956](#)
- On QFX10002, QFX10008, and QFX10016, an automatically correcting, nonfatal hardware error on the PE chip (which is the ASIC on PTX1000, PTX10002, and QFX10002, on the the third-generation FPC on PTX3000 and PTX5000, and on the line card on PTX10008, PTX10016, QFX10008, and QFX10016) is reported as a fatal error and thus the related Packet Forwarding Engine gets disabled. The code changes have been made to change the error category from **FATAL** to **INFO** to avoid the Packet Forwarding Engine to be disabled unexpectedly. [PR1408012](#)
- On QFX5000 platforms with **flexible-ethernet-services** enabled, when **family inet/inet6** and **vlan-bridge** are configured on the same physical interface, and **family inet/inet6** is configured first, MAC address movement (MAC learning/deleting) might not happen on this interface. This might cause a traffic drop. [PR1408230](#)
- There is a possibility of seeing multiple reconnect logs, **JTASK_IO_CONNECT_FAILED**, during the device initialisation. There is no functionality impact because of these messages. These messages can be ignored. [PR1408995](#)
- Intermittently chassis alarms not raised after the device is power cycled. . Chassis alarms can be recovered by restarting lcmd the CLI - with the **request app-engine service restart chassis-manager** or, **restart chassis-control**. [PR1413981](#)
- During normal operation, if the **chassis-control** process restarts, ASICs are not initialized. As a result, the packet drops are seen on the output queue. [PR1414434](#)
- When a virtual-switch routing instance is created, the QFX10,000 Packet Forwarding Engine need to allocate a VLAN context for it for MAC lookup. This VLAN context is required only for the virtual-switch routing instance. It is not required for routing instance of instance type EVPN, because only SP-style interfaces are supported on routing instances of instance type EVPN. The scale of VLAN context allocation is limited in QFX10000 Packet Forwarding Engine so, it needs a flag to indicate that the rtt is of instance type EVPN specifically. QFX10000 uses RTT_FLAGS_PROTO-EVPN, which is set based on VPLS_RTF_PROTO_EVPN. However, VPLS_RTF_PROTO_EVPN is set in the control plane when the rtt instance type is EVPN, or when **protocol evpn mpls** is configured. This causes problem for the default-switch routing instance when **protocol evpn encap mpls** is configured, and in some scenarios, the VLAN context is not allocated for the default-switch routing instance. Based on the discussion with

the Packet Forwarding Engine team, the fix is to add a specific VPLS_RTf_xx flag in rtb_extended_prflags, and QFX10000 Packet Forwarding Engine might pick it up used in the VLAN context allocation logic. [PR1416987](#)

- On QFX5110 and QFX5120 platforms, uRPF check in strict mode might not work properly. [PR1417546](#)
- On the QFX10000 line of devices, if an analyzer is configured to mirror traffic of an input aggregated Ethernet interface and a new member is added to the same aggregated Ethernet interface, then the analyzer might not provide sample packets that flow through a newly added child interface. [PR1417694](#)
- For transit static LSPs, QFX5120-48Y/QFX5120-32C devices might end up in swapping with an invalid label instead of POP/PHP action, which might result in packet drop in the adjacent LER node. Because the chipset used in the QFX5120 has additional capabilities for MPLS, this issue is applicable only to QFX5120-48Y/QFX5120-32C platforms and not applicable to other platforms. As a workaround, removing and reapplying the static transit LSP configuration solves this issue. [PR1420370](#)
- Packets of size greater than the maximum transfer unit (MTU) of a GRE interface are not fragmented. [PR1420803](#)
- On QFX5120-32C, the DHCP binding on the client might fail when the QFX5120-32C acts as the DHCP server. This is seen only for channelized ports. For non-channelized port (40-Gbps or 100-Gbps), this issue is not seen. [PR1421110](#)
- When channelization is configured on FPC QFX10000-30C (ULC-30Q28) while J-Flow (J-Flow v9 or v10) is configured on this board, the J-Flow export might fail. The issue results in loss of sample flow. [PR1423761](#)
- When first FPC is down, ping does not work. [PR1423928](#)
- This issue happens when two primary addresses are configured on the lo0 interface and one is removed later. In this case, all IFBDs are removed and added back because of **static vtep** configuration. RG-ID of BD is reset and MAC synchronization does not happen. This happens for a few VLANs only. [PR1424013](#)
- More number of MACs/MAC-IP addresses can be learned if **mac/mac-ip** limit is configured in a particular sequence. An example is shown below: 1. Learn 50 remote entries 2. Configure a MAC limit of 20 (remote entries remain intact, this works as expected) 3. Learn 50 local entries. At this point, no local entries must be learned, as the MAC limit is 20. However, all 50 local MAC addresses are learned, causing the MAC count to be 100, which is incorrect. The same issue is seen for MAC-IP limit as well. [PR1428572](#)
- Hardware is not getting programmed on rebooting QFX5000 node for CoS rewrite on aggregated Ethernet (LAG) interfaces. [PR1430173](#)
- Sometimes a filter is not attached to the interface even though it exists in the configuration. [PR1430385](#)
- When NSSU is done from Junos OS Release 18.1R3 to any forwarded image on QFX5100 Virtual Chassis with LACP link protection configuration, there might be around 5 minutes of traffic loss. Traffic loss is not seen during NSSU if link protection configuration is not present. [PR1435519](#)
- The dcpfe process generates a core file after NSSU upgrade of backup QFX5200 and reboot of QFX5200 when it is going down. Once the reboot is complete the dcpfe process is up and stable. [PR1435963](#)

- On QFX5000 platforms, transit DHCPv6 packets might be dropped. That is, pass through DHCPv6 packets might not be forwarded. [PR1436415](#)
- An IPv6 firewall filter applied to egress interface sometimes does not work after multiple reconfiguration and ends up dropping all IPv6 traffic. [PR1438202](#)
- Unified ISSU fails from Junos OS Release 17.2X75-D4x to Junos OS Release 19.2R1 might not be supported on QFX5200. [PR1438690](#)
- When lacp is configured with link protection and force-up on local, and peer is configured with link protection, disabling the active member on peer device causes LACP MUX state to be stuck in attached state. Issue is not seen if link protection is not configured on the peer device. The feature where link protection and force-up is configured on local and link protection is configured on peer is not qualified. It is mention in release note, so that it can be documented. [PR1439268](#)
- Control logical interface 16386 on channelized interfaces might not get recreated after in-service system reboot. This impacts the LLDP functionality. [PR1439358](#)
- NDI cannot be used in VLAN with IRB on EX92XX. Neighborhood advertisements or solicit packets destined to host are getting dropped with NDI inspection (under DHCPv6 security) on a VLAN with IRB configuration on EX92XX in Junos OS Release 18.4 and later. [PR1439844](#)
- Because of excessive back to back unified ISSU or ISSR looks like FS corruption happens (mount/umount), and backup Routing Engine synchronization takes abnormal longer time causing system to be unstable. In this case, a unified ISSU abort is expected and it is recommended to reboot the system. [PR1442490](#)

Layer 2 Ethernet Services

- On QFX5100 or QFX5200 line of switches with spine-leaf scenario, when some (two or more than two) underlay interfaces with ECMP are brought down on leaf devices, the multihop BFD overlay sessions between spines and leafs might flap. And if BFD flaps, the protocols depending on BFD (typically, IBGP protocol) might also flap, which leads to traffic impact. [PR1416941](#)

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20--50 ms traffic drop on the existing logical interface. [PR1367488](#)
- On a QFX5100 Q-in-Q might stop working for certain VLAN ID list configured under a physical interface. This is result of a Packet Forwarding Engine binary issue which is addressed through an upcoming image. [PR1395312](#)
- On QFX Series platform where the Layer 3 virtual extensible LAN (VXLAN) gateway is supported such as QFX5110, stale entries might be observed if route change happens, triggering route and next hop deletion on Packet Forwarding Engine. Because of the increasing stale entries, which might further fill

up the corresponding table and causes the new entries to not get added successfully, traffic loss might be observed as a result. [PR1423368](#)

- Multiple QFX Series platforms might be unable to commit baseline configuration after zeroization.
{master:0}[edit] root# commit check Mar 26 05:50:48 mustd: UI_FILE_OPERATION_FAILED: File /var/run/db/enable-process.data doesn't exist Mar 26 05:50:48 mgd[1938]:
UI_FILE_OPERATION_FAILED: Failed to open /var/run/db/enable-process.data+ file error: Failed to open /var/run/db/enable-process.data+ file error: configuration check-out failed: daemon file propagation failed. [PR1426341](#)
- CRC errors might be seen when other manufacturer device is connected to QFX10000 on a 100-Gigabit link with QSFP-100GBASE-LR4-T2. Other manufacturer device report CRC errors and input errors on those 100-Gigabit links. The QFX10000 interfaces do not show any errors. It might cause packet loss. [PR1427093](#)
- On QFX5000 platforms, the FPC crashes when a firewall filter is applied on a logical unit of a DSC interface. This issue has traffic impact. [PR1428350](#)
- There might be a traffic loss of approximately 10 seconds with LACP link protection configuration during NSSU. [PR1431034](#)
- The dcpfe crashes and unified ISSU fails from Junos OS Release 17.2X75-D4x to Junos OS Release 19.2R1 and does not support QFX5200. [PR1440288](#)
- In Junos OS Release 19.2R1, traffic do not flow when IRB over aggregated Ethernet is configured as from interface match criteria for a firewall filter. [PR1441230](#)

MPLS

- The time lapse between interface-down interrupt detection to FRR callback is approximately 148 ms on the QFX5110 platform, though the in-place update FRR programming completes in 1 ms. The minimum FRR time achieved with this limitation is approximately 150 ms and maximum is approximately 275 ms. [PR1440344](#)

Platform and Infrastructure

- In configurations with IRB interfaces, during times of interface deletion (for example, FPC reboot), the Packet Forwarding Engine might log errors stating **nh_ucast_change:291Referenced l2ifl not found**. This condition should be transient, with the system reconverging on the expected state. [PR1054798](#)

Routing Protocols

- On QFX5100 switches, the FXPC core files are generated after the IS-IS overload bit is reconfigured. [PR1123116](#)
- Firewall filter should not be applied on VXLAN mapped VLAN on QFX5000 platform is not supported in Junos OS Release 18.4R1. Also, **user-vlan-id match condition** is not supported for filter which is applied to vxlan enabled interface. [PR1398237](#)
- On QFX-5100 VC/VCF, the following error is observed: **BRCM_NH-,brcm_nh_bdvlan_ucast_uninstall(), 128:I3 nh 6594 unintsall failed in h/w** with mini-PDT base configurations. There is no functionality impact because of this error message. [PR1407175](#)
- In BGP graceful restart scenario, including helper mode which is enabled by default, rdp might generate a core file because of the improper handling of BGP graceful restart stale routes during the deletion of BGP neighbors. The rpd might crash and service or traffic impact might occur. [PR1427987](#)

SEE ALSO

[What's New | 177](#)

[What's Changed | 186](#)

[Known Limitations | 188](#)

[Resolved Issues | 197](#)

[Documentation Updates | 204](#)

[Migration, Upgrade, and Downgrade Instructions | 205](#)

[Product Compatibility | 219](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 19.2R1](#) | **197**

This section lists the issues fixed in Junos OS Release 19.2R1 for the QFX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper online [Junos Problem Report Search](#) application.

Resolved Issues: 19.2R1

IN THIS SECTION

- [Authentication and Access Control](#) | **198**
- [Class of Service \(CoS\)](#) | **198**
- [EVPN](#) | **198**
- [General Routing](#) | **198**
- [Interfaces and Chassis](#) | **202**
- [Junos Fusion Satellite Software](#) | **202**
- [Layer 2 Features](#) | **202**
- [Layer 2 Ethernet Services](#) | **203**
- [Network Management and Monitoring](#) | **203**
- [Routing Protocols](#) | **203**
- [Spanning Tree Protocols](#) | **203**

Authentication and Access Control

- Without configuring anything related to dot1x, the syslog **dot1xd[2192]: task_connect: task PNACAUTH./var/run/authd_control addr /var/run/authd_control: Connection refused** is generated repeatedly. [PR1406965](#)

Class of Service (CoS)

- Error message **STUCK_BUFF : port_sp not empty for port 35 sp 1 pkts:1**. [PR1346452](#)

EVPN

- The rpd process might crash with EVPN type-3 route churn. [PR1394803](#)
- EVPN routes might show **Route Label: 0** in addition to the real label. [PR1405695](#)
- The rpd might crash after an NSR switchover in an EVPN scenario. [PR1408749](#)
- ARP entry is still pointing to the failed VTEP after the PE-CE link fails for a multihomed remote ESI. [PR1420294](#)
- Multicast MAC addresses being learned in the Ethernet switching table with VXLAN through an ARP packet in a pure L2 configuration. [PR1420764](#)
- The device might proxy the ARP probe packets in an EVPN environment. [PR1427109](#)
- Extra incorrect MAC move might be seen when the host moves continuously between the different ESIs. [PR1429821](#)
- ESI is configured on a single-homed 25-gigabit port might not work. [PR1438227](#)

General Routing

- The 1-gigabit copper module interface shows **Link-mode: Half-duplex** on the QFX10000 line of devices. [PR1286709](#)
- Interface flap on 100GBASE-LR4 is seen during an unified ISSU. [PR1353415](#)
- On QFX5120 switches, the convergence delay between PE1 and P router link is more than the expected delay value. [PR1364244](#)
- RIPv2 update packets might not be sent when **IGMP snooping** is enabled. [PR1375332](#)
- The **overlay-ecmp** configuration might not work as expected on QFX5110 in an EVPN-VXLAN environment. [PR1380084](#)
- There is an inconsistency in applying a scheduler map with **excess-rate** on the physical interface and the aggregated Ethernet interface. [PR1380294](#)
- Traffic get silently dropped and discarded When the FPC is taken offline in an MC-LAG scenario. [PR1381446](#)
- Last reboot reason is incorrect if the device is rebooted because of power cycling. [PR1383693](#)
- Disable reporting of correctable single-bit error on Hybrid Memory Cube (HMC) and prevent the major alarm. [PR1384435](#)

- The configuration statement **show chassis errors active detail** is not supported on QFX5000 platforms. [PR1386255](#)
- The rpd and KRT queue get stuck in a VRF scenario. [PR1386475](#)
- ARP received on an SP-style interface is not sent to all RVTEPs in case of QFX5100 Virtual Chassis only; the normal BUM traffic works fine. [PR1388811](#)
- The input rate (in pps) do not increase on EX2300-MP uplink ports when the packet is a pure L2 packet such as non-etherII or non-EtherSnap. [PR1389908](#)
- 10-gigabit copper link flapping might happen during a TISSU operation of QFX5100-48T switches. [PR1393628](#)
- **BRCM_NH-,brcm_bcm_mpls_tunnel_initiator_clear(),226:bcm_mpls_tunnel_initiator_get failed intf = 4 failure** error logs might seen in syslog. [PR1396014](#)
- On QFX5110 Fan LED turns amber randomly. [PR1398349](#)
- The interrupt process consumes high CPU because of the `intr{swi4: clock (0)}` on QFX5100-48t-6Q running a QFX5100 Series image and Junos OS Release 18.x code. [PR1398632](#)
- The DHCPv6 relay packets are dropped when both the UDP source and destination ports are 547. [PR1399067](#)
- CPU hog might be observed on the QFX10000 line of switches. [PR1399369](#)
- The DHCPv6 relay-reply packet might be dropped by the DHCP relay. [PR1399683](#)
- PEM I2C failure alarm might be shown incorrectly as failed. [PR1400380](#)
- MAC limit with persistent MAC is not working after reboot. [PR1400507](#)
- On QFX5120-32C error logs for flex counter are seen with GRE configuration. [PR1400515](#)
- Only one Packet Forwarding Engine might be disabled on FPC with multiple Packet Forwarding Engines in error/wedge condition. [PR1400716](#)
- File permissions are changed for `/var/db/scripts` files after reboot. [PR1402852](#)
- The DHCP discover packets are forwarded out of an interface incorrectly if **DHCP snooping** is configured on that interface. [PR1403528](#)
- The VRRP VIP might not work when it is configured on the LAG interface. [PR1404822](#)
- Commit warning message is seen on QFX5100 switches. [PR1405138](#)
- Executing the **request system configuration rescue save** command might fail with error messages. [PR1405189](#)
- DHCP does not work for some clients in dual Junos fusion aggregated device setup on extended ports (EP). [PR1405495](#)
- VXLAN transit traffic over tagged underlay L3 interface and underlay IRB interface gets dropped because of the hardware limitation. [PR1406282](#)

- The ARP request might not be resolved successfully if **arp-suppression** is enabled and **vlan-id-list** is configured on the QFX10000 node. [PR1407059](#)
- The DHCP discover packets might be dropped over VXLAN tunnel if DHCP relay is enabled for other VXLAN or VLANs. [PR1408161](#)
- MAC address movement might not happen in flexible Ethernet services mode when family inet/inet6 and vlan-bridge are configured on the same physical interface. [PR1408230](#)
- Fan failure alarms might be seen on QFX5100-96S after upgrading to Junos OS Release 17.3R1. [PR1408380](#)
- Restarting the line card on QFX10008 and QFX10016 with MC-LAG enhanced-convergence might cause intra-VLAN traffic to get silently dropped and discarded. [PR1409631](#)
- The FPC might crash and might not come up if the interface number or next hop is set to maximum value under **vlan-routing** on QFX Series platforms. [PR1409949](#)
- LLDP memory leak when IEEE dcbx packet is received in auto-negotiation mode followed by another dcbx packet with none of ieee_dcbx TLVs present. [PR1410239](#)
- On EX2300-24P, error message **dc-pfe: BCM_NH-,brcm_nh_resolve_get_nexthop(),346:Failed to find if family.** [PR1410717](#)
- Fix jfirmware support to upgrade primary BIOS from a system booted from secondary BIOS. [PR1411603](#)
- Traffic loss might be observed after VXLAN configuration change. [PR1411858](#)
- The spfe on satellite device in Junos fusion setup might crash and it might cause the satellite device to go offline. [PR1412279](#)
- PEM alarm for a backup FPC will remain on the master FPC though the backup FPC is detached from Virtual Chassis. [PR1412429](#)
- Junos PCC might reject PCUpdate or PCCreate message if there is a metric type other than type 2. [PR1412659](#)
- On QFX5000 line of switches, the EVPN/VXLAN mutlicast next-hop limit is 4000. [PR1414213](#)
- VC ports using DAC might not establish a link on QFX5200. [PR1414492](#)
- DC output information is missing in the **show chassis environment pem** output for whitebox. [PR1414703](#)
- VXLAN encapsulation next hop (VENH) does not get installed during BGP flap or restart routing. [PR1415450](#)
- FEC change from FEC91 to NONE does not take effect on 100-gigabit Ethernet interfaces with QSFP-100GBASE-SR4 optics. [PR1416376](#)
- Two instances of Junos OS are running after an upgrade to Junos OS Release 18.1R3-S3.7. [PR1416585](#)
- On restarting routing, the dcpfe might generate a core file at **nh_composite_change**. [PR1416925](#)
- ERSPAN traffic does not tag when output interface is trunk port. [PR1418162](#)

- Traffic loss might be seen on the aggregated Ethernet interface on QFX10000 platforms. [PR1418396](#)
- Rebooting QFX5200-48Y using **request system reboot** does not take physical links offline immediately. [PR1419465](#)
- On QFX5120-48Y or QFX5120-32C, 100-gigabit PSM4 optics connected ports went down randomly. [PR1419826](#)
- Ping fails over type-5 tunnel on IRB interfaces under EVPN-VXLAN scenario. [PR1420785](#)
- Error messages might be seen on QFX10000 platforms during DFE tuning. [PR1421075](#)
- On QFX5120-32C, DHCP binding on client might fail when QFX5120-32C acting as DHCP server is seen only for channelized port. [PR1421110](#)
- ETS configuration does not apply on non cascade ports when the AD is rebooted. [PR1421429](#)
- BFD might get stuck in slow mode on QFX10002, QFX10008, and QFX10016 platforms. [PR1422789](#)
- QFX5100-48T 10-Gbps interface might be auto negotiated at 1-Gbps speed instead of 10-Gbps. [PR1422958](#)
- The interface cannot get up when the **remote-connected interface** only supports 100M in QFX5100 VC setup. [PR1423171](#)
- BUM traffic coming over IRB underlay interface gets dropped on destination VTEP in a PIM-based VXLAN. [PR1423705](#)
- Traffic drops when an FPC reboots with aggregated Ethernet member links deactivated by a remote device. [PR1423707](#)
- Ping over EVPN type-5 route to QFX10000 does not work. [PR1423928](#)
- All interfaces will be down and the dcpfe might crash if SFP-T is inserted in a QFX5210. [PR1424090](#)
- IPv6 neighbor solicitation packets for link-local address are dropped when passing through QFX10002-60C. [PR1424244](#)
- QFX5120 QSFP-100G-PSM4 interfaces are undetected and come back up as channelized interfaces. [PR1424647](#)
- All interfaces creation fails after NSSU. [PR1425716](#)
- Heap memory leak might be seen on QFX10000 platforms. [PR1427090](#)
- On QFX5120-48Y, the interfaces with the QSFP-100GBASE-ER4L optics do not come up in Junos OS Release 18.3R1-S2.1. [PR1428113](#)
- The configuration statement **show chassis environment** shows **Input0** and **Input1**. [PR1428690](#)
- The l2ald process crashes and generates a core file when the number of VXLAN HW IFBDS exceeds the maximum limit of 16,382. [PR1428936](#)
- An interface on a QFX Series switch does not come up after the transceiver is replaced with one having different speed. [PR1430115](#)

- When the IRB interface is trying to broadcast an ARP request, the ARP request might not go out of the chip because of the SDK bug, which might lead to ARP failure in QFX5120. [PR1430327](#)
- On QFX Series switches, the **Validation of meta data files failed** message is seen on the hypervisor. [PR1431111](#)
- Transit DHCPv6 packets might be dropped on QFX5000 platforms. [PR1436415](#)

Interfaces and Chassis

- Changing the value of **mac-table-size** to default might lead all FPCs to reboot. [PR1386768](#)
- Missing mandatory ICCP configuration statement **redundancy-group-id-list** produces a misleading error message. [PR1402606](#)
- EVPN aggregated Ethernet interface flap followed by a commit. [PR1425339](#)

Junos Fusion Satellite Software

- Extended port (EP) LAG might go down on the satellite devices (SDs) if the related cascade port (CP) links to an aggregation device (AD) goes down. [PR1397992](#)

Layer 2 Features

- On QFX Series switches, the error message **Failed with error (-7) while deleting the trunk 1 on the device 0** is seen. [PR1393276](#)
- QFX5000 - symmetric hash. [PR1397229](#)
- On QFX5000, dcpfe process crash might be observed during restart of the Packet Forwarding Engine on a system with scaled EVPN/VXLAN configuration. [PR1403305](#)
- On QFX Series EVPN-VXLAN, the unicast IPv6 NS message gets flooded on L3GW. Both IPv4 and IPv6 traffic gets dropped on L2SW. [PR1405814](#)
- The IPv6 NS/NA packets received over VTEP from an ESI host are incorrectly flooded back to the host. [PR1405820](#)
- **IGMP-snooping** on EVPN-VXLAN might impact OSPF hello packets flooding after a VTEP leaf reboot. [PR1406502](#)
- With cut through configuration enabled after the device is rebooted, cut through mode is disabled on the channelized interfaces in releases before Junos OS Release 19.1R1. [PR1407706](#)
- QFX5110 Virtual Chassis generates DDOS messages of different protocols on inserting a 1-gigabit or 10-gigabit SFP transceiver or after forming a VCP connection. [PR1410649](#)
- With **arp-suppression** enabled, QFX5000 might not forward IPv6 router solicitations or advertisements packets. [PR1414496](#)

Layer 2 Ethernet Services

- The malfunction of the core isolation feature in EVPN-VXLAN scenarios causes traffic to get silently dropped and discarded. [PR1417729](#)

Network Management and Monitoring

- The chassisd might crash and restart after the AGENTX session timeout between master (snmpd) and subagent times out. [PR1396967](#)
- Log files might not get compressed during the upgrade. [PR1414303](#)

Routing Protocols

- Host-destined packets with **filter log** action might reach the Routing Engine. [PR1379718](#)
- BUM packets might get looped if EVPN multihoming interfaces flap. [PR1387063](#)
- EVPN-VXLAN NON-COLLAPSED AUTONEG errors and flush operation failed errors are seen after the device is power cycled. [PR1394866](#)
- On QFX5110 and QFX5200, EVPN-VXLAN NON-COLLAPSED state, dcpfe generates a core file at `brcm_pkt_tx_flush`, `l2alm_mac_ip_timer_handle_expiry_event_loc` after a random event. [PR1397205](#)
- The FPC/dcpfe process might crash because of the interface flapping. [PR1408428](#)
- ERACL firewall group operates in double wide mode for QFX5110 in Junos OS Release 19.1R1. [PR1408670](#)
- Host-generated ICMPv6 RA packets might be dropped on the backup member of Virtual Chassis if **igmp-snooping** is configured. [PR1413543](#)
- The QFX Series switches might not install all IRB MAC addresses in the initialization. [PR1416025](#)
- After an IRB logical interface is deleted, MAC entry for the IRB interface is deleted for the IRB hardware address; as a result, packets destined to other IRB logical interfaces where MAC is not configured are impacted. [PR1424284](#)

Spanning Tree Protocols

- The l2cpd might crash if the VSTP traceoptions and VSTP VLAN all commands are configured. [PR1407469](#)

SEE ALSO

[What's New | 177](#)

[What's Changed | 186](#)

[Known Limitations | 188](#)

[Open Issues | 190](#)

[Documentation Updates | 204](#)

Documentation Updates

IN THIS SECTION

- [Installation and Upgrade guide | 204](#)

This section lists the errata and changes in Junos OS Release 19.2R1 for the QFX Series switches documentation.

Installation and Upgrade guide

- **Veriexec explained (QFX Series)**—Verified Exec (also known as veriexec) is a file-signing and verification scheme that protects the Junos operating system (OS) against unauthorized software and activity that might compromise the integrity of your device. Originally developed for the NetBSD OS, veriexec was adapted for Junos OS and enabled by default from Junos OS Release 7.5 onwards.

[See [Veriexec Overview](#).]

SEE ALSO

What's New 177
What's Changed 186
Known Limitations 188
Open Issues 190
Resolved Issues 197
Migration, Upgrade, and Downgrade Instructions 205
Product Compatibility 219

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrading Software on QFX Series Switches | 205
- Installing the Software on QFX10002-60C Switches | 208
- Installing the Software on QFX10002 Switches | 208
- Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches | 209
- Installing the Software on QFX10008 and QFX10016 Switches | 211
- Performing a Unified ISSU | 215
- Preparing the Switch for Software Installation | 216
- Upgrading the Software Using Unified ISSU | 216
- Upgrade and Downgrade Support Policy for Junos OS Releases | 218

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrading Software on QFX Series Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For information about the contents of the jinstall package and details of the installation process, see the [Installation and Upgrade Guide](#) and [Junos OS Basics](#) in the QFX Series documentation.

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to <https://www.juniper.net/support/downloads/junos.html>.

The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.
3. Select **19.2** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 19.2 release.

An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

NOTE: We recommend that you upgrade all software packages out of band using the console, because in-band connections are lost during the upgrade process.

Customers in the United States and Canada use the following command:


```
user@host> request system software add
source/jinstall-host-qfx-5-x86-64-19.2-R1.n-secure-signed.tgz reboot
```

Replace **source** with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the switch.
- For software packages that are downloaded and installed from a remote location:
 - **ftp://hostname/pathname**
 - **http://hostname/pathname**
 - **scp://hostname/pathname** (available only for Canada and U.S. version)

Adding the **reboot** command reboots the switch after the upgrade is installed. When the reboot is complete, the switch displays the login prompt. The loading process can take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.



NOTE: After you install a Junos OS Release 19.2 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-x.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add <pathname><source>** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-19.2R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add <pathname><source>** command.

For example:

```
user@switch> request vmhost software add
ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-19.2R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

If the installation package resides locally on the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-f-x86-64-19.2R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-19.2R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add <pathname><source>** command.

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add <pathname><source> re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at <https://www.juniper.net/support>.



WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

```
user@switch# delete chassis redundancy
```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate  
/var/tmp/jinstall-host-qfx-10-f-x86-64-19.2R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

9. Reboot the switch to start the new software using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete <package-name>** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

```
user@switch> show version
```

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
Slot 0:
  Current state           Backup
  Election priority       Master (default)
Routing Engine status:
Slot 1:
  Current state           Master
  Election priority       Backup (default)
```

14. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate
/var/tmp/jinstall-host-qfx-10-f-x86-64-19.2R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the [CLI Explorer](#).

15. Reboot the Routing Engine using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall <package-name>** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the **show version** command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state           Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state           Backup
    Election priority       Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 216](#)
- [Upgrading the Software Using Unified ISSU on page 216](#)

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

To verify that nonstop active routing is enabled:

NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

```
user@switch> show task replication
Stateful Replication: Enabled
RE mode: Master
```

If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information about how to enable it.

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the **request system snapshot** command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Installing Software Packages on QFX Series Devices*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
 - On the switch, enter:

```
user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
```

where *package-name.tgz* is, for example, *jinstall-host-qfx-10-f-x86-64-18.3R1.n-secure-signed.tgz*.

NOTE: During the upgrade, you cannot access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get
lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
```

```

ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases

provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 17.1, 17.2 and 17.3 are EEOL releases. You can upgrade from Junos OS Release 17.1 to Release 17.2 or from Junos OS Release 17.1 to Release 17.3.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

SEE ALSO

[What's New | 177](#)

[What's Changed | 186](#)

[Known Limitations | 188](#)

[Open Issues | 190](#)

[Resolved Issues | 197](#)

[Documentation Updates | 204](#)

[Product Compatibility | 219](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 219](#)

Hardware Compatibility

To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on QFX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://apps.juniper.net/feature-explorer/>.

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the [Hardware Compatibility tool](#).

SEE ALSO

What's New		177
What's Changed		186
Known Limitations		188
Open Issues		190
Resolved Issues		197
Documentation Updates		204
Migration, Upgrade, and Downgrade Instructions		205

Junos OS Release Notes for SRX Series

IN THIS SECTION

- [New and Changed Features](#) | [221](#)
- [Changes in Behavior and Syntax](#) | [231](#)
- [Known Behavior](#) | [233](#)
- [Known Issues](#) | [235](#)
- [Resolved Issues](#) | [237](#)
- [Documentation Updates](#) | [245](#)
- [Migration, Upgrade, and Downgrade Instructions](#) | [246](#)
- [Product Compatibility](#) | [247](#)

These release notes accompany Junos OS Release 19.2R1 for the SRX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

New and Changed Features

IN THIS SECTION

- [New and Changed Features: 19.2R1-S1 | 222](#)
- [New and Changed Features: 19.2R1 | 222](#)

This section describes the new features and enhancements to existing features in Junos OS Release 19.2R1 for the SRX Series devices.

New and Changed Features: 19.2R1-S1

Routing Protocols

- **Decouple RSVP for IGP-TE (MX Series, PTX Series, ACX Series, QFX Series, SRX Series, and EX Series)**—Starting in Junos OS Release 19.2R1-S1, device can advertise selective **traffic-engineering** attributes such as **admin-color** and **maximum-bandwidth**, without enabling RSVP, for segment routing and interior gateway protocol (IGP) deployments.

New and Changed Features: 19.2R1

Application Security

- **Application-based multipath support (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX4100, SRX4200, and vSRX)**—Starting in Junos OS Release 19.2R1, application-based multipath routing is supported on SRX Series devices.

Multipath routing allows the sending device to create copies of packets and to send each copy through two or more WAN links. On the other end, multipath calculates the jitter and packet loss for the combined links and estimates the jitter and packet loss for the same traffic on individual links. You can compare the reduction in packet loss when combined links instead of individual links are used. Sending multiple copies of traffic ensures timely delivery of the sensitive application traffic.

Multipath support in SD-WAN use cases enhances application experience.

[See [Application Quality of Experience](#).]

- **Application-level logging for AppQoE (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX4100, SRX4200, and vSRX)**—Starting in Junos OS Release 19.2R1, SRX Series devices support application-level logging for AppQoE. This feature reduces the impact on the CSO or log collector device while processing a large number of system log messages generated at the session-level. The SRX Series device maintains session-level information and provides system log messages for the session level. Replacing session-level logging with application-level logging decreases the overhead on the SRX Series device and increases AppQoE throughput.

[See [AppQoE](#).]

- **Secure Web proxy (SRX Series and vSRX)**—Starting in Junos OS Release 19.2R1, SRX Series devices support secure Web proxy service.

The secure Web proxy feature enables you to specify dynamic Web applications for which the system performs proxy service. In this deployment, the SRX Series device receives a request from the client, examines the HTTP header for the application, and redirects the request directly to the webserver based on the application.

As a result, the SRX Series device performs transparent proxy between the client and the webserver for the specified applications and provides better quality of service for the application traffic.

[See [SSL Proxy](#).]

- **Application identification of micro-applications (SRX Series, vSRX)**—Starting in Junos OS Release 19.2R1, SRX Series devices support micro-applications with the application identification (AppID) feature.

AppID detects the applications at the subfunction level on your network and the security policy leverages the application identity information determined from the AppID module. After a particular application is identified, an action such as permit, deny, reject, or redirect is applied to the traffic according to the policy configured on the device.

[See [Application Identification](#).]

- **JDPI-Decoder engine version upgrade (SRX Series)**—Starting in Junos OS Release 19.2R1, the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine comes with a default application signature package version 999 that includes the protobundle version 1.380.0-64.005 and the JDPI-Decoder engine version 5.3.0-56. You can also upgrade the application signature package when a new signature package version is available.

[See [show services application-identification status](#).]

Flow-Based and Packet-Based Processing

- **PowerMode IPsec fragment support (SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 19.2R1, PowerMode IPsec (PMI) is enhanced to handle the incoming and outgoing fragment packets in first path or fast path processing.

PMI supports first path and fast path processing both for fragment handling and for unified encryption. You can enable PowerMode IPsec processing by using the **set security flow power-mode-ipsec** command.

See [[Improving IPsec Performance with PowerMode IPsec](#).]

- **Multiple J-Flow Server (SRX Series)** —On SRX Series devices, the J-Flow version 9 can export flow records to only one collector. Starting from Junos OS Release 19.2R1, the J-Flow version 9 can configure up to 4 collectors under a family.

Packet Forwarding Engine exports flow record, flow record template, option data, and option data template packet to up to four collectors under a family. The template that is mapped, and the export version across the collectors under a family should be same.

- **Per-flow CoS support for GTP-U in PMI mode (SRX5000 line of devices with SPC3)**— Starting in Junos OS Release 19.2R1, Junos OS supports per-flow CoS functions for GTP-U traffic in PowerMode IPsec (PMI) mode. This feature introduces tunnel endpoint identifier (TEID)-based hash distribution for creating GTP-U sessions to multiple cores on the anchor PIC when both PMI and IPsec session affinity are enabled. TEID-based hash distribution helps split a fat GTP session into multiple slim GTP sessions and process them on multiple cores in parallel. With this enhancement, per-flow CoS for GTP-U traffic is enabled even when the traffic carries multiple streams with different DSCP code within one GTP tunnel.

[See [PMI Flow Based CoS functions for GTP-U](#).]

Intrusion Detection and Prevention (IDP)

- **Support for IDP intelligent inspection (SRX Series and vSRX)**—Starting in Junos OS Release 19.2R1, you can enable IDP intelligent inspection and tune it dynamically to reduce IDP inspection load. IDP intelligent inspection helps the device to recover from overload state when the configured CPU and memory threshold values exceed the resource limits. Prior to Junos OS Release 19.2R1, when the device exceeds the configured CPU and memory threshold limit, IDP either rejects or ignores new sessions.

[See [IDP Intelligent Inspection](#).]

Juniper Sky ATP

- **Juniper Sky ATP Support for Encrypted Traffic Inspection and Server Name Identification**—Starting in Junos OS 19.2, SRX Series devices support inspection of encrypted traffic (HTTPS) in security-intelligence policies. Server name identification (SNI) checks are also supported. Note that these changes do not introduce any new CLI commands. All existing commands and configurations can make use of this expanded functionality.

Junos Telemetry Interface

- **Support for JTI (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 19.2R1, you can stream statistics through junos telemetry interface (JTI) to an outside collector using remote procedure call (gRPC) services. gRPC is a protocol for configuration and retrieval of state information.

JTI supports the following sensors:

- Log messages (resource path `/junos/events`)
- Border Gateway Protocol (BGP) peer information (resource path `/network-instances/network-instance/protocols/protocol/bgp/`)
- Memory utilization for a routing protocol task (resource path `/junos/task-memory-information/`)
- Operational state of hardware components (resource path `/components/`)
- Operational state of the AE interface (resource path `/lACP/`)
- Operational state of Ethernet interfaces enabled with Link Layer Discovery Protocol (LLDP) (resource path `/lldp/`)
- Address Resolution Protocol (ARP) statistics (resource path `/arp-information/`)
- Routing Engine internal interfaces, such as `fxp0`, `em0`, and `em1` (resource path `/interfaces/interface[name=' interface-name ']/`)
- Network Discovery Protocol (NDP) table state (resource path `/nd6-information/`)
- NDP router advertisement statistics (resource path `/ipv6-ra/`)

- Intermediate System to Intermediate System (IS-IS) protocol statistics (resource path / **network-instances/network-instance/protocols/protocol/isis/levels/level/**)
- IS-IS protocol (resource path /**network-instances/network-instance/protocols/protocol/interfaces/interface isis/levels/level/**)

[See [Guidelines for gRPC Sensors \(Junos Telemetry Interface\)](#).]

J-Web

- **Threats Map (Live) (SRX Series except SRX5000 line of devices and vSRX)**—Starting in Junos OS Release 19.2R1, you can monitor Threat Maps (Live). You can view blocked and allowed threat events based on feeds from intrusion prevention systems (IPSs), antivirus, antispam engines, Juniper Sky ATP, and screen options. You can also choose a country and view the total threat events for that country since midnight, followed by the number of inbound and outbound threat events, and see the top five IP addresses, either inbound or outbound. With View Details, you can see the additional details of the selected country.

[See [Monitor Threats Map \(Live\)](#).]

- **Quick Setup wizard enhancement (SRX Series except SRX5000 line of devices)**—Starting in Junos OS Release 19.2R1 after the configuration is completed, you see a notification message when you access J-Web again through a new browser tab or window with the configured IPv4 or IPv6 address.

[See [Understanding the J-Web CLI Terminal](#).]

Getting Started panel (SRX Series)—Starting in Junos OS Release 19.2R1, you have quick access to the important configurations using a Getting Started panel on the J-Web UI. For logical systems users and tenant users, this option is available only in SRX1500, SRX4100, SRX4200, SRX4600, and SRX5000 line of devices.

By default, this panel appears when you log in. If you choose **Don't show this again**, then you can access this panel using the help (?) icon.

[See [Security J-Web Getting Started](#).]

- **HA Mode wizard (SRX Series)**—Starting in Junos Release 19.2R1, you can configure chassis cluster using a new HA Mode wizard when the devices are in factory default. You can create HA using the same wizard from Configure > Device Settings > Cluster (HA) Setup when the devices are already in the network.

[See [Configuring Cluster \(HA\) Setup](#).]

- **IPS Sensor enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, you can configure IP Sensor using the following settings:
 - Basic—Supports protection mode, IDP intelligent inspection, and basic IDP flow configuration.
 - Advanced—Supports IDP flow, global, IPS, log, reassembler, and packet log configuration.
 - Detectors settings—Supports the configuration for a specific service. You can also add or edit the configuration inline.

[See [Sensor Configuration Page Options](#).]

- **Active Directory enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX, and for the SRX5000 and SRX300 lines of devices, you can configure the integrated user firewall in a maximum of two domains. For the other SRX Series devices, you can create only one domain.

[See [Configuring Active Directory](#).]

- **Certificate management enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, you can now configure device certificates, trusted certificate authorities (CAs), and CA groups. You can view information about the local certificate, trusted CA profiles, and CA groups that are configured on the device. You can manually generate self-signed certificate. You can enroll online, export, import, manually load, and delete the local certificate or certificate signing request (CSR).

[See [Managing Device Certificates](#).]

- **Forwarding mode enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, flow mode is the default mode for processing traffic. You can now configure an SRX Series devices as a border router by changing the flow-based processing to packet-based processing.

[See [Forwarding Configuration Page Options](#).]

- **Dashboard enhancement (SRX Series except SRX5000 line of devices)**—Starting in Junos OS 19.2R1, you can view the Web filtering, Antispam, Content filtering, Application & Users, and Threat monitoring widgets in the J-Web dashboard for root, logical systems, and tenant users.

[See [Monitoring the Dashboard](#).]

- **Security policy rules enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, when you create rules for the destination traffic, you can:
 - Add an application or application group for a dynamic application using the Add New Application/Group button.
 - Add a service for Service(s) using the Add New Service button.

[See [Configuring Firewall Security Policy Rules](#).]

Monitoring firewall events enhancement (SRX Series except SRX5000 line of devices)—Starting in Junos OS Release 19.2R1, you can now see that an application displays the same value as a nested application (if the application supports nested applications).

[See [Monitoring Firewall Events](#).]

- **Monitoring events enhancement (SRX Series except SRX5000 line of devices)**—Starting in Junos OS Release 19.2R1, you can monitor the following new events:
 - ATP—Top Malware Source Countries, Infected File Categories, and Malwares Identified widgets are shown in the chart view and detailed advanced anti-malware (AAMW) logs are shown in the grid view.
 - Security Intelligence—Top Infected Hosts and C&C Servers widgets are shown in the chart view and detailed secintel logs are shown in the grid view.

- Screens—Top Screen Attacks, Screen Victims, and Screen Hits widgets are shown in the chart view and detailed screen logs are shown in the grid view.

[See [Monitoring ATP Events](#), [Monitoring Security Intelligence Events](#), and [Monitoring Screen Events](#).]

- **Juniper Sky ATP enrollment enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, you can view the detailed enrollment steps on the SKY ATP Enrollment page.

[See [Sky ATP Enrollment](#).]

- **Link aggregation enhancement (Standalone SRX Series)**—Starting in Junos OS Release 19.2R1, VLAN tagging is enabled by default when you add an AE interface.

[See [Link Aggregation Configuration Page Options](#).]

- **OSPF enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, you can configure OSPF area in two ways:

- Basic—You can add new routing instances.
- Advanced—You can group a policy and trace options.

[See [OSPF Configuration Page Options](#).]

- **VLAN enhancement (SRX Series)**—Starting in Junos OS Release 19.2R1, Bridge domain is the new name for VLANs in Layer 2 transparent mode. You can assign an interface for the created VLANs. You can view all the available VLANs with their IDs, interfaces assigned, and status.

[See [VLAN Configuration Page Options](#).]

Logical Systems and Tenant Systems

- Starting in Junos OS Release 19.2R1, the following features that are supported on the logical systems are now extended to tenant systems:

- **Default routing-instance support for tenant systems (SRX Series)**—Starting in Junos OS Release 19.2R1, you can use the **ping**, **telnet**, **ssh**, **traceroute**, **show arp**, **clear arp**, **show ipv6 neighbors**, and **clear ipv6 neighbors** commands to pass the virtual router configured in a tenant system as a default routing instance.

[See [Tenant Systems Overview](#).]

- **UTM support for tenant systems (SRX Series)**—Starting in Junos OS Release 19.2R1, SRX Series devices support unified threat management (UTM) on tenant systems. Use the **set utm default-configuration** command under the **[edit security]** hierarchy level to create a default UTM profile for tenant systems. Configure policies, profiles, and custom objects for each tenant system in the UTM profile.

[See [UTM for Tenant Systems](#).]

- **On-box logging support for tenant systems (SRX Series)**—Starting in Junos OS Release 19.2R1, SRX Series devices support on-box logging configurations for each tenant system, and handle logs based on these configurations. Configure the **set log mode event** and **set log mode stream** commands under

the **[edit security]** hierarchy level to enable on-box logging. Tenant systems also support binary format log in event mode.

[See [Security Log for Tenant Systems](#).]

- **IDP for tenant systems (SRX Series and vSRX)**—Starting in Junos OS Release 19.2R1, tenant systems support intrusion detection and prevention (IDP). The IDP policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a tenant system.

[See [IDP for Tenant Systems](#).]

Network Management and Monitoring

- **Support for displaying valid user input in the CLI for command options and configuration statements in custom YANG data models (SRX Series)**—Starting in Junos OS Release 19.2R1, the CLI displays the set of possible values for a given command option or configuration statement in a custom YANG data model when you include the **action-expand** extension statement in the option or statement definition and reference a script that handles the logic. The **action-expand** statement must include the **script** child statement, which defines the Python action script that is invoked when a user requests context-sensitive help in the CLI for the value of that option or statement.

[See [Displaying Valid Command Option and Configuration Statement Values in the CLI for Custom YANG Modules](#).]

Security

- **Support to configure micro-applications in a unified policy (SRX Series and vSRX)**—Starting in Junos OS Release 19.2R1, you can configure micro-applications in a unified policy. Micro-applications are subfunctions of a particular application.

You can configure micro-applications at the same hierarchy as predefined dynamic applications in a security policy and take the action based on the policy rules.

[See [Configuring Micro-Applications in Unified Policies](#).]

Unified Threat Management (UTM)

- **SRX5K-SPC3 support Avira scan engine on antivirus module (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 19.2R1, SRX Series devices support an on-device antivirus Avira scan engine. The on-device antivirus Avira scan engine scans the data by accessing the virus pattern database. The antivirus scan engine is provided as a unified threat management (UTM) module that you can download and install on an SRX Series device either manually or by using the Internet to connect to a Juniper Networks-hosted URL or a user-hosted URL.

NOTE: The SRX5000 line of devices with SRX5K-SPC-4-15-320 or SRX5K-SPC-2-10-40 cards do not support the on-device antivirus Avira scan engine.

[See [On-Device Antivirus Scan Engine](#).]

VPN

- **PIM using point-to-multipoint mode support for AutoVPN and Auto Discovery VPN (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, and vSRX)**—Starting in Junos OS Release 19.2R1, Protocol Independent Multicast (PIM) using point-to-multipoint (P2MP) mode supports AutoVPN and Auto Discovery VPN in which a new **p2mp** interface type is introduced for PIM. The **p2mp** interface tracks all PIM joins per neighbor to ensure that multicast forwarding or replication happens only to those neighbors that are in joined state. In addition, the PIM using point-to-multipoint mode supports chassis cluster mode.

[See [Multicast Overview](#), [Understanding AutoVPN](#), [Understanding Auto Discovery VPN](#), and [Understanding Multicast Routing on a Chassis Cluster](#).]

- **PowerMode IPsec for NAT-T (SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 19.2R1, SRX Series devices equipped with SRX5K-SPC3 Services Processing Cards (SPCs) support PowerMode IPsec (PMI) for Network Address Translation-Traversal (NAT-T).

[See [Understanding PowerMode IPsec](#).]

- **IPsec Distribution Profile (SRX5400, SRX5600, and SRX5800)**—Starting with Junos OS Release 19.2R1, you can manage the tunnel distribution through the configuration. You can create a profile for a VPN object to handle the distribution of tunnels. In a profile, mention the slot and thread-id where the tunnels from the VPN object should be distributed. The same profiles can be used for different VPN objects.

To add profiles for distributing IPsec SAs, use the new **distribution-profile profile-name** statement.

[See [IPsec Distribution Profile](#) and [distribution-profile](#).]

- **Anti-replay window (SRX Series 5000 line of devices with SPC3 cards)**—Starting from Junos OS Release 19.2R1, you can configure the anti-replay window size within the range of 64 to 8192 (power of 2). If you do not configure the anti-replay window size, the default window size remains as 64.

To configure the window size, use the new **anti-replay-window-size** option.

[See [Replay Protection](#).]

SEE ALSO

[What's Changed | 231](#)

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

[Product Compatibility | 247](#)

Changes in Behavior and Syntax

IN THIS SECTION

- [Application Security | 232](#)
- [Ethernet Switching and Bridging | 232](#)
- [Flow-Based and Packet-Based Processing | 232](#)
- [Network Management and Monitoring | 232](#)
- [VPNs | 233](#)

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 19.2R1 for the SRX Series.

Application Security

- Starting in Junos OS Release 19.2R1, the SSL decryption mirroring feature is supported on redundant Ethernet (reth) interface on SRX Series devices operating in a chassis cluster.

Ethernet Switching and Bridging

- **Support for double tagged VLANs being pushed out the egress interface (SRX300, SRX320, SRX340, SRX345, SRX550, and SRX1500)**—Starting in Junos OS Release 19.2R1, in a Q-in-Q scenario, double tagged VLANs are pushed out the egress interface. In previous releases, when two VLANs were added at the ingress interface, with the **native-vlan-id *vlan-id*** assigned to the user-to-network interface (UNI) interface and the **vlan-id *vlan-id-list*** assigned to the network-to-network interface (NNI) interface, the VLAN with the **native-vlan-id** tag did not exit from the egress interface. Now both VLAN tags exit from the egress interface.

Flow-Based and Packet-Based Processing

- **Power Mode IPsec (SRX Series)**—On SRX Series devices, when Power Mode IPsec is enabled, the **show security flow statistics** and **show security flow session tunnel summary** commands does not count, or display the number of packets that are processed within the Power Mode IPsec as these packets do not go through the regular flow path.

[See [show security flow statistics](#)]

Network Management and Monitoring

- **The show system schema command and <get-yang-schema> RPC require specifying an output directory (SRX Series)**—Starting in Junos OS Release 19.2R1, when you issue the **show system schema** operational mode command in the CLI or execute the **<get-yang-schema>** RPC in a remote session to retrieve schema files, you must specify the directory in which to generate the output files by including the **output-directory** command option in the CLI or the **<output-directory>** element in the RPC. In earlier releases, you can omit the **output-directory** argument when requesting a single module to display the module in standard output.
- **Custom YANG RPC support for input parameters of type empty (SRX Series)**—Starting in Junos OS Release 19.2R1, custom YANG RPCs support input parameters of type **empty** when executing the RPC's command in the Junos OS CLI, and the value passed to the action script is the parameter name. In earlier releases, input parameters of type **empty** are only supported when executing the RPC in a NETCONF or Junos XML protocol session, and the value passed to the action script is the string '**none**'.

[See [Creating Action Scripts for YANG RPCs on Devices Running Junos OS](#).]

- **NSD Restart Failure Alarm (SRX Series)**—Starting in Junos OS Release 19.2R1, a system alarm is triggered when the Network Security Process (NSD) is unable to restart due to the failure of one or more NSD

subcomponents. The alarm logs about the NSD are saved in the messages log. The alarm is automatically cleared when NSD restarts successfully.

The **show chassis alarms** and **show system alarms** commands are updated to display the following output when NSD is unable to restart - **NSD fails to restart because subcomponents fail**.

[See [Alarm Overview](#).]

VPNs

- **Certificate revocation list (SRX Series)**—Local certificates are being validated against certificate revocation list (CRL) even when CRL check is disabled. Starting in Junos OS Release 19.2R1, this can be stopped by disabling the CRL check through the Public Key Infrastructure (PKI) configuration. When CRL check is disabled, PKI will not validate local certificate against CRL.

[See [revocation-check \(Security PKI\)](#) and [Understanding Online Certificate Status Protocol and Certificate Revocation Lists](#).]

SEE ALSO

[What's New | 221](#)

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

[Product Compatibility | 247](#)

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 19.2R1 for the SRX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Flow-Based and Packet-Based Processing

- A maximum of 250 Web proxy profile creations are supported in Junos OS 19.2R1 release on all SRX Series devices. [PR1428495](#)

J-Web

- CLI terminal is not working in Java version 1.8 due to security restriction in running applet. [PR1341956](#)
- After generating Default Trusted CA profile group (Local) under Certificate Management>Trusted Certificate Authority in J-Web, it does not display CA profile group **Local** under Certificate Management>Certificate Authority Group page. [PR1424131](#)
- The imported ca-profile-group using J-Web will not populate the group in the Certificate Authority Group initial landing page grid, but all the ca-profiles of a group will be populated under Trusted Certificate Authorities landing page. [PR1426682](#)
- Country logo is not displaying in **Threats Map** page and **Events** page for some countries. Time slider is not displayed properly in **Screen/ATP/Security Intelligence** events pages. [PR1435124](#)

VPNs

- The HA design in SRX, anti-replay window is synced to the backup only when the total incoming packet count is an odd multiple of 128 packets. When a failover occurs, the anti-replay bitmap is not synced. Again, when the node comes back online, the SA is installed but anti-replay bitmap is reset to 0 along with In and out sequence number. [PR1420521](#)
- On SRX Series devices, when st0 interface IP address is changed, both IKE and IPsec SAs might go down [PR1422630](#)

SEE ALSO

[What's New | 221](#)

[What's Changed | 231](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

[Product Compatibility | 247](#)

Known Issues

IN THIS SECTION

- [Chassis Clustering](#) | 235
- [Flow-Based and Packet-Based Processing](#) | 235
- [J-Web](#) | 236
- [Platform and Infrastructure](#) | 236
- [User Firewall](#) | 236
- [VPNs](#) | 236

This section lists the known issues in hardware and software in Junos OS Release 19.2R1 for SRX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Chassis Clustering

- When GTP profile with the same name is deleted and then added, the profile ID will be changed. So, if this profile is being used by policy, you need to reconfigure the policy application bounding; otherwise, the GTP will not work as you expect. [PR1409213](#)

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices with SPC3, it is possible when multiple cores occur in quick succession, that the coldsync monitored status is displayed and cannot be removed even though coldsync has finished. User will be required to reboot the affected node to recover. [PR1403000](#)
- On the SRX5000 line of devices, when the cluster only has a single SPC card in each node, if the SPC2/SPC3 card goes offline in the primary node, a split brain might occur. This could cause traffic loss. Reboot both nodes to recover from this issue. [PR1403872](#)
- GRE traffic through the IPsec tunnel will be dropped after routing is restarted. [PR1423768](#)
- On SRX1500 platform, when interface is changed from access mode to MVRP trunk port, traffic will be blocked and dynamic VLAN can't be learned. As a workaround, reboot the device or srxpfe after configuration, or by change access mode to trunk mode first, then change to MVRP trunk port. [PR1438153](#)

J-Web

- Due to **set chassis auto-image-upgrade** in **factory-config**, from **phone home** page we are not able to **skip to J-Web** with error **Bootstrap is in progress, Can't Skip!!**. [PR1420888](#)
- **SECINTEL_ACTION_LOG** events with subcategories such as **Infected-Hosts** and **C&C** are not shown on Juniper Sky ATP threat count on **Monitor>Threats Map** page in J-Web. [PR1425795](#)

Platform and Infrastructure

- When internal SA is enabled, and reboot/upgrade one node 0, then wait 90 seconds to reboot/upgrade another node, system may not come online. As a workaround, reboot both nodes at the same time to recover. [PR1423169](#)
- When maintenance endpoint of connectivity fault management (CFM) is used and a link defect event (for example, the link goes down) happens, **FMD_CCM_DEFECT_RMEP** and **CFMD_CCM_DEFECT_NONE** (few minutes later than **FMD_CCM_DEFECT_RMEP**) log messages will be observed accordingly. Because **CFMD_CCM_DEFECT_NONE** indicates that the defect has been cleared, though actually it has not, in this situation, it is a misleading message. If event policy is configured and matches **CFMD_CCM_DEFECT_NONE**, some actions might be taken automatically and finally impact traffic (for example, incorrect failover of links). [PR1427493](#)
- On SRX4600 platform when manual RGO failover is performed, sometimes node0 (the original primary node) stays in secondary-hold status for long time and cannot change back to secondary status. [PR1421242](#)
- On high scaled environment, there could be very rare scenario where you can observe a vmcore in TCP stack (tcp_respond). This is due to platform optimization. [PR1444764](#)

User Firewall

- Some sqlite db files in **/var/db/userid/** may be corrupted after the whole box is rebooted. When the issue happened, the userfw feature cannot work. As a workaround, remove all related db files and restarted useridd and jqsyncd to restore userfw feature. [PR1442369](#)

VPNs

- VPN does not recover on the high-end standalone SRX Series devices when CLI operation **restart ipsec-key-management** is done. [PR1390831](#)
- IKE SAs are not displayed in CLI output after failover happens on a cluster node when tunnels are established in aggressive mode. [PR1424077](#)
- On SRX5000 Series devices with SPC3, when IPsec lifetime and reauth lifetime coincide, then IPsec SA gets filled with multiple IPsec SAS. [PR1430389](#)

- On SRX5000 Series devices with SPC3 card plugged in, sometimes VPN tunnel does not come up after changing configuration from IPv4 to IPv6 tunnels. [PR1431265](#)
- On SRX5000 Series devices with SPC3, sometimes IPsec tunnel may not come up after configuration is changed from responder-only to **responder-only-no-rekey ikev1**. [PR1441320](#)

SEE ALSO

[What's New | 221](#)

[What's Changed | 231](#)

[Known Limitations | 233](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

[Product Compatibility | 247](#)

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 19.2R1 for SRX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Application Firewall

- Fail to match permit rule in Application Firewall (AppFW) rule set. [PR1404161](#)

Application Identification

- IDP install failing on secondary node due to AI installation failure. [PR1336145](#)

Application Layer Gateways (ALGs)

- DNS requests with the EDNS option might be dropped by the DNS ALG. [PR1379433](#)
- On all SRX Series platforms, SIP/FTP ALG does not work when SIP traffic with source NAT goes through the SRX Series devices. [PR1398377](#)

- The TCP rst packet is dropped when any TCP proxy-based feature and **rst-invalidate-session** are enabled simultaneously. [PR1430685](#)

Chassis Clustering

- The SNMP trap sends wrong info with **Manual failover**. [PR1378903](#)
- Traffic with domain name address might fail for 3-5 minutes after RG0 failover on SRX Series platforms. [PR1401925](#)
- The flowd process stops when updating or deleting a GTP tunnel. [PR1404317](#)
- Mixed mode (SPC3 coexisting with SPC2 cards) high availability (HA) IP-Monitoring fails on secondary node with **secondary arp entry not found** error [PR1407056](#)
- The SRX Series devices might be potentially overwritten with an incorrect buffer address when detailed logging is configured under the GTPv2 profile. [PR1413718](#)
- Starting with Junos OS Release 18.4, at most, 6 pdn connects can be contained in a pdp context response; otherwise, the response will be dropped. [PR1422877](#)
- Memory leaks might be seen on the jsqsyncd process on SRX chassis clusters [PR1424884](#)
- RG0 failover sometimes causes FPC offline/present status. [PR1428312](#)

Flow-Based and Packet-Based Processing

- Control traffic loss may be seen on SRX4600 platform. [PR1357591](#)
- On SRX1500 devices, the activity LED (right LED) for 1-Gigabit Ethernet/10G-Gigabit Ethernet port is not on although traffic is passing through that interface. [PR1380928](#)
- Password recovery menu is not shown up on SRX device. [PR1381653](#)
- Large file downloads slow down for many seconds. [PR1386122](#)
- On the SRX300 line of devices default configuration changed. [PR1393683](#)
- Switching interface mode between family **ethernet-switching** and **family inet/inet6** might cause traffic loss. [PR1394850](#)
- SRX to not strip vlan added by native vlan id command. [PR1397443](#)
- Increase DAG feed scale number to 256 from 63. [PR1399314](#)
- CPU is hitting 100 percent with fragmented traffic. [PR1402471](#)
- On SRX5400, SRX5600, and SRX5800 devices with SPC3, when PowerMode IPsec is enabled, the **show security flow statistics** and **show security flow session tunnel summary** commands will not count or display the number of packets processed within PowerMode IPsec, because these packets do not go through regular flow path. [PR1403037](#)

- Downloads might stall and/or completely fail when utilizing services that are reliant on TCP proxy. [PR1403412](#)
- The flowd process stops and all cards are brought offline. [PR1406210](#)
- The RG1 failover does not happen immediately when the SPC3 card crashes. [PR1407064](#)
- The flowd process might crash if **enable-session-cache** knob is configured under the SSL termination profile. [PR1407330](#)
- Support for LAG interface with PowerMode IPsec. [PR1407231](#)
- The kernel might stop on the secondary node when committing **set system management-instance** command. [PR1407938](#)
- On SRX1500 platform, traffic is blocked on all interfaces after configuring **interface-mac-limit** on one interface. [PR1409018](#)
- Memory leak if AAMW is enabled. [PR1409606](#)
- Packets might get dropped in chassis cluster Z mode with local interface configured. [PR1410233](#)
- Session capacity of SRX340 does not match SRX345. [PR1410801](#)
- While PMI is ON, IPsec encrypted statistics on the Routing Engine **show security ipsec statistics** are not working anymore for fragment packets. [PR1411486](#)
- PEM 0 or PEM 1 or FAN, I2C failure major alarm might be set and cleared multiple times. [PR1413758](#)
- HA packets might be dropped on SRX5000 line of devices with IOC3 or IOC2 cards. [PR1414460](#)
- On SRX1500, SRX4100, SRX4200, SRX4600, and SRX5000 line of devices with SPC3 card, if SSL proxy is configured, the firewall FPC CPU might spike above 80 percent and traffic might be lost. [PR1414467](#)
- Any traffic originated from the device itself might be dropped in the IPsec tunnel. [PR1414509](#)
- The input and output bytes or bps statistic values might not be identical for the same size of packets. [PR1415117](#)
- The reth interfaces are now supported when configuring SSL decryption mirroring (**mirror-decrypt-traffic interface**) [PR1415352](#)
- Force clearing **Client Session** from flow does not clean up **Proxy session**. [PR1415756](#)
- Traffic would be dropped if SOF is enabled in a chassis cluster in active/active mode. [PR1415761](#)
- Juniper Sky ATP does not escape the \ inside the username before the metadata is sent to the cloud. [PR1416093](#)
- The flowd process stops on the SRX5000 Series or SRX4000 lines of devices when large-size packets go through IPsec tunnel with the post-fragment check. [PR1417219](#)
- TCP segmented client side session fails to create transparent proxied relay session, and session stays idle. [PR1417389](#)
- Best path selected keeps changing at regular intervals even when no violation is reported. [PR1417926](#)

- Traffic might be lost on the SRX Series device if IPsec session affinity is configured with **ipsec-performance-acceleration** command. [PR1418135](#)
- Group VPN IKE security-associations can not establish before RG0 failover. [PR1419341](#)
- On all SRX Series devices firewalls, if the traffic-log feature is configured, logs might incorrectly display IPv4 addresses in an IPv6 format [PR1421255](#)
- The **show security flow session session-identifier < sessID>** is not working if the session ID is bigger than 10M on SRX4600 platform. [PR1423818](#)
- The tunnel-id information is displayed in the flow session. [PR1423889](#)
- Replace **bypass-on-dns-cache-miss** command with **drop_on_dns_error** command in Web proxy profile. If **drop_on_dns_error** command is not set and DNS failure occurs for a session, that session passes through bypass mode. If **drop_on_dns_error** command is set and DNS failure occurs for a session, that session is dropped by Web proxy plug-in. [PR1430425](#)
- Support IPv6 session through Web proxy. [PR1433088](#)
- The applications which get declassified in the middle of session will not be identified properly. [PR1437816](#)
- Partial traffic might get dropped on an existing LAG. [PR1423989](#)
- Alarms due to high temperature when operating with expected temperatures. [PR1425807](#)
- PIM neighbors might not come up on SRX Series chassis cluster [PR1425884](#)
- The IPsec traffic going through SRX5000 line of devices with SPC2 cards installed causes SPU CPU utilization to be high. [PR1427912](#)
- Uneven distribution of CPU with high PPS on device. [PR1430721](#)
- SRX550M running Junos OS Release 18.4R1 shows PEM 1 output failure message where as with Junos OS Release 15.1X49 or Junos OS Release 18.1R3.3 it does not show any alarms. [PR1433577](#)
- Some webpages cannot be fully rendered. [PR1436813](#)

Infrastructure

- Increase in Junos OS image size for Junos OS Release 19.1R1. [PR1423139](#)

Interfaces and Routing

- On SRX4600 platform, the 40-Gigabit Ethernet might flap continuously by MAC local fault. [PR1397012](#)
- SRX Series devices cannot obtain IPv6 address through DHCPv6 when using a PPPoE interface with a logical unit number greater than 0. [PR1402066](#)

Intrusion Detection and Prevention (IDP)

- IDP might crash with the custom IDP signature. [PR1390205](#)
- Unable to configure **dynamic-attack-group** command. [PR1418754](#)

Installation and Upgrade

- ISSU failed from Junos OS Release 18.3R1.9 to Junos OS Release 18.4R1.4. [PR1405556](#)
- SRX1500 devices running Junos OS Release 15.1X49-D160 are unable to be upgraded or downgraded successfully to all releases built before 17 February 2019 [PR1407556](#)

J-Web

- In the J-Web dashboard, the **Security Resources** widget did not display absolute values. [PR1372826](#)
- J-Web now supports defining SSL-Proxy and redirect (block page) profiles when a policy contains dynamic applications. [PR1376117](#)
- Configuring using the CLI editor in J-Web generates an mgd core file. [PR1404946](#)
- The httpd-gk process stops, leading to dynamic VPN failures and high Routing Engine CPU utilization (100 percent). [PR1414642](#)
- Risk report, when generated in IE browser, appears completely out of alignment and XML tags are displayed. [PR1415767](#)
- J-Web configuration change for an address set using the search function results in a commit error. [PR1426321](#)
- J-Web not working when logged in as read-only user. [PR1428520](#)
- IRB interface is not available in zone option of J-Web. [PR1431428](#)

Logical Systems and Tenant Systems

- Tenant system administrator can change vlan assignment beyond the allocated tenant system. [PR1422058](#)

Multiprotocol Label Switching (MPLS)

- RPD might restart unexpectedly when **no-cspf** is configured and lo0 is not included under protocol rsvp. [PR1366575](#)

Network Address Translation (NAT)

- SRX SPC3 mix mode, NAT SPC3 core files are generated at `../sysdeps/unix/sysv/linux/raise.c:55`. [PR1403583](#)

Network Management and Monitoring

- The **set system no-redirects** setting does not take effect for the reth interface. [PR894194](#)
- The chassisd might crash and restart after the AGENTX session timeout between master(snmpd) and sub-agent. [PR1396967](#)

Platform and Infrastructure

- In chassis cluster redundancy group failover scenario, on SRX5600 and 5800 platforms, if the failover is caused by interface monitoring failure, the failover on Packet Forwarding Engine side (that is, data plane) might be slow (for example, impact on BFD session up to several seconds). This issue might result in protocol and traffic outage. [PR1385521](#)
- The flowd process might crash if there are too many IPsec tunnels [PR1392580](#)
- Complete device outage might be seen when an SPU VM core file is generated. [PR1417252](#)
- Some applications might not be installed during upgrade from lower version which does not support FreeBSD 10 to FreeBSD 10(based system). [PR1417321](#)
- On SRX Series devices, flowd process stops might be seen. [PR1417658](#)
- Routing Engine CPU utilization is high and eventd process is consuming a lot of resources. [PR1418444](#)
- On SRX4600 device, commit failed while configuring 2047 VLAN IDs on the reth interface. [PR1420685](#)

Routing Policy and Firewall Filters

- Memory leak in nsd prevents change from taking effect. [PR1414319](#)
- The flowd process (responsible for traffic forwarding in SRX Series devices) stops on SRX Series devices while deleting a lot of policies from Junos Space. [PR1419704](#)
- A commit warning will now be presented to the user when a traditional policy is placed below a unified policy. [PR1420471](#)
- The dynamic-address summary's IP entry count does not include IP entries in root logical system. [PR1422525](#)
- If restarting NSD fails, there is no any indication or symptom, and users don't know it. So a new alarm is added to indicate this failure. [PR1422738](#)
- The ipfd generates a core file while scaling cases 6-1. [PR1431861](#)

Unified Threat Management (UTM)

- Whitelist/blacklist does not work for HTTPS traffic going through Web proxy. [PR1401996](#)
- On SRX Series devices, when configuring Enhanced Web Filtering on the CLI, the autocomplete function did not properly handle or suggest custom categories. [PR1406512](#)
- On SRX Series devices, when using Unified Policies and Web filtering (EWF) without SSL proxy, the Server Name Indication (SNI) might not be identified correctly and the RT_UTM logs were recording incomplete information. [PR1410981](#)
- Unable to achieve better Avira AV TP on SRX4600 due to reaching mbuf high watermark. [PR1419064](#)
- UTM Web filtering status shows down when using Hostname [routing-instance synchronization failure]. [PR1421398](#)
- When using Unified Policies, the base-filter for certain UTM profiles might not be applied correctly. [PR1424633](#)
- The custom-url-categories are now pushed correctly to the Packet Forwarding Engine under all circumstances. [PR1426189](#)

User Interface and Configuration

- Tenant system administrator cannot view the configuration with **Empty Database** message when configuring tenant system using **groups**. [PR1422036](#)

VPNs

- On SRX1500 device, when configuring IPsec VPN and BGP simultaneously, the kmd process might stop and generate a core file if BGP peers reach approximately 350. All of the VPN tunnels will be disconnected during the pause. [PR1336235](#)
- SPC3 IKE SA detail output is not showing proper traffic statistics. [PR1371638](#)
- The pkid process might stop after RG0 failover. [PR1379348](#)
- On SRX5400, SRX5600, and SRX5800 devices with SPC3, the **show security ike security-association detail** command does not display local IKE-ID field correctly. [PR1388979](#)
- A few VPN tunnels do not forward traffic after RG1 failover. [PR1394427](#)
- The kmd process might stop when SNMP polls for the IKE SA. [PR1397897](#)
- VPN tunnels flap after adding or deleting a configuration group in edit private mode on a clustered setup. [PR1400712](#)
- Syslog is not generated when IKE gateway rejects duplicate IKE ID connection. [PR1404985](#)
- Idle IPsec VPN tunnels without traffic and with ongoing DPD probes can be affected during RG0 failover. [PR1405515](#)
- Not all the tunnels are deleted when authentication algorithm in IPsec proposal is changed. [PR1406020](#)
- On SRX5400, SRX5600, and SRX5800 devices with SPC3, the incoming packet's flow context information is not reset correctly when the packet is dropped in IPsec acceleration module. This will cause subsequent packets to be incorrectly processed as IPsec packets and results in the crash. To address this issue, SRX Series device now resets the flow context before dropping the packet in all relevant modules including IPsec acceleration module. [PR1407910](#)
- On SRX5400, SRX5600, and SRX5800 devices with SPC3, when SRX Series device is configured in IKEv1 and NAT traversal is active, after a successful IPsec rekey, IPsec tunnel index might change. In such a scenario, there might be some traffic loss for a few seconds. [PR1409855](#)
- Traffic drops on peer due to bad SPI after first reauthentication. [PR1412316](#)
- On SRX5400, SRX5600, and SRX5800 devices with SPC3, when SRX Series device is configured to initiate IKEv2 reauthentication when NAT traversal is active, occasionally reauthentication may fail. [PR1414193](#)
- The flowd/srxpfe process might stop when traffic selector is used for IPsec VPN [PR1418984](#)

- The **show security ike sa detail** command shows incorrect value in **IPSec security associations** column. [PR1423249](#)
- On SRX5000 Series devices with SPC3, with P2MP and IKEv1 configured, if negotiation fails on the peer device, then multiple IPSec SA entries are created on the device if the peer keeps triggering new negotiation. [PR1432852](#)
- On SRX Series devices with SPC3, should send IKE delete notification to peer when traffic selector configuration is changed for a specific AutoVPN. [PR1426714](#)
- The kmd process stops and generates a core file after running the **show security ipsec traffic-selector** command. [PR1428029](#)
- IPsec rekey triggers for when sequence number in AH and ESP packet is about to exhaust is not working. [PR1433343](#)

SEE ALSO

[What's New | 221](#)

[What's Changed | 231](#)

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

[Product Compatibility | 247](#)

Documentation Updates

There are no errata or changes in Junos OS Release 19.2R1 documentation for the SRX Series.

SEE ALSO

[What's New | 221](#)

[What's Changed | 231](#)

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths. You can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 15.1X49, 17.3, 17.4, 18.1, and 18.2 are EEOL releases. You can upgrade from one Junos OS Release to the next release or one release after the next release. For example you can upgrade from Junos OS Release 15.1X49 to Release 17.3 or 17.4, Junos OS Release 17.4 to Release 18.1 or 18.2, and from Junos OS Release 18.1 to Release 18.2 or 18.3 and so on.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

For information about software installation and upgrade, see the [Installation and Upgrade Guide for Security Devices](#).

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

SEE ALSO

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Product Compatibility | 247](#)

Product Compatibility

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

SEE ALSO

[What's New | 221](#)

[What's Changed | 231](#)

[Known Limitations | 233](#)

[Open Issues | 235](#)

[Resolved Issues | 237](#)

[Documentation Updates | 245](#)

[Migration, Upgrade, and Downgrade Instructions | 246](#)

Upgrading Using ISSU

In-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

For additional information about using ISSU on routing and switching devices, see the [High Availability User Guide](#).

For additional information about using ISSU on security devices, see the [Chassis Cluster User Guide for SRX Series Devices](#).

For information about ISSU support across platforms and Junos OS releases, see the [In-Service Software Upgrade \(ISSU\)](#) Web application.

Licensing

Starting in 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program is a framework, set of policies, and tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that have been developed at Juniper Networks over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information on the list of supported products, see [Juniper Flex Program](#).

Compliance Advisor

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

Finding More Information

- **Feature Explorer**—Determine the features supported on MX Series, PTX Series, QFX Series devices. The Juniper Networks Feature Explorer is a Web-based app that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. <https://pathfinder.juniper.net/feature-explorer/>
- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved. prsearch.juniper.net.
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. apps.juniper.net/hct/home

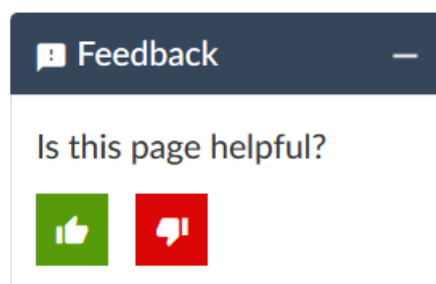
NOTE: To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products. apps.juniper.net/compliance/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://support.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.juniper.net/support/>
- Search for known bugs: <https://kb.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://support.juniper.net/support/downloads/>

- Search technical bulletins for relevant hardware and software notifications:
<https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://forums.juniper.net>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
<https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at
<https://support.juniper.net/support/requesting-support/>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at <https://www.juniper.net/documentation/feedback/>.

Revision History

22 April 2021—Revision 14, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

13 January 2021—Revision 13, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

9 July 2020—Revision 12, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

14 May 2020—Revision 11, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 March 2020—Revision 10, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

2 January 2020—Revision 9, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

28 November 2019—Revision 8, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

8 November 2019—Revision 7, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

31 October 2019—Revision 6, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

6 September 2019—Revision 5, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

26 July 2019—Revision 4, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

12 July 2019—Revision 3, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

4 July 2019—Revision 2, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.

27 June 2019—Revision 1, Junos OS Release 19.2R1— ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, and Junos Fusion.